



cezurity

Антивирусный Сканер Cezurity

Руководство по установке и использованию

v3.0

Содержание

Описание Сканера	1
Основные возможности и преимущества	1
Что может нанести вред компьютеру и данным	1
Как работает Антивирусный Сканер Cezurity	2
Установка и удаление Сканера	3
Системные требования	3
Установка Антивирусного Сканера	3
Удаление Сканера	5
Работа Сканера	6
Управление Сканером и панель настроек	6
Участие в программе Cezurity Cloud	8
Типы проверки компьютера	8
Результаты проверок	9
Лечение заражений	11
Журнал событий	12
Часто задаваемые вопросы (FAQ)	13
Контактная информация и техническая поддержка	15

Описание Сканера

Основные возможности и преимущества

- Обнаружение всех типов вредоносных программ, включая вирусы, трояны, шпионское ПО, вредоносные расширения браузеров, руткиты.
- Обнаружение сложных вредоносных программ, заражающих систему на уровне, близком к аппаратному.
- Лечение заражений.
- Быстрая проверка компьютера займет несколько минут, так как не требуется скачивать вирусные базы.
- Бесплатно.

Что может нанести вред компьютеру и данным

Степень опасности обнаруженных программ может быть разной. Если одни программы являются заведомо вредоносными, то другие могут использоваться вами осознанно, либо обладать лишь потенциальной возможностью нанести какой-то вред. В зависимости от типа и опасности обнаруженным объектам присваиваются различные статусы.

Классификация	Обозначение	Определение
Вредоносная программа	 Malware	Программы, намеренно созданные для выполнения несанкционированных действий на компьютере пользователя. Как правило, такие действия наносят вред – это может быть кража данных, мошенничество, загрузка или запуск других вредоносных программ, кража аккаунтов и пр. Типичными вредоносными программами являются вирусы, черви, трояны.
Инфицированные файлы	 Infected	Легитимные файлы, которые были заражены. В отличие от вредоносных программ (Malware) их нельзя просто удалить – это может привести к нестабильности работы операционной системы и приложений.
Нежелательное ПО	 Unwanted	Программное обеспечение, которое нельзя однозначно отнести к вредоносному, но оно способно так или иначе навредить пользователю. Например, это могут быть шпионские или рекламные программы. Пользователи иногда сами загружают и устанавливают такое ПО, не понимая, какие именно функции оно выполняет. Часто вредоносные функции являются дополнением к тем, которые нужны пользователям.
Потенциально опасное ПО	 Riskware	Программы, сами по себе не являющиеся вредоносными, но их функции или особенности могут использоваться злоумышленниками в корыстных целях. Например, это ПО для удаленного администрирования, средства защиты авторских прав (DRM), различные утилиты.



По умолчанию Сканер обнаруживает опасность всех типов, кроме “Потенциально опасного ПО” (Riskware). Это сделано для того, чтобы случайно не оказались удалены легитимные программы (т. е. программы, которые вы установили сами и используете осознанно). Включить детектирование потенциально опасного ПО можно на панели настроек в окне на **локальном компьютере** – см. пункт “Управление Антивирусным Сканером и панель настроек”.

Как работает Антивирусный Сканер Cezurity

Антивирусный Сканер Cezurity – это бесплатный облачный сервис для обнаружения активных вредоносных программ и лечения заражений. Антивирусный Сканер разработан и поддерживается компанией Cezurity.

Сканер можно установить на зараженный компьютер, чтобы его вылечить. Кроме того, Сканер поможет убедиться в отсутствии заражения на компьютере. Например, вы можете запускать проверку каждый раз перед тем, как заплать через интернет или войти в онлайн-игру. Антивирусный Сканер совместим с антивирусами и полезен для того, чтобы получить второе мнение о том, не заражен ли компьютер.

Антивирусный Сканер – это новое поколение средств борьбы с вредоносными программами. Раньше антивирусы выполняли ряд проверок, направленных на поиск зараженных файлов на компьютере. Для этого файлы на компьютере сравнивались с образцами вредоносного кода (сигнатурами, определениями вредоносных объектов). Антивирусная программа искала, нет ли в файлах на компьютере совпадений с базой вирусов. Если такое совпадение обнаруживалось, объект признавался вредоносным. То есть, общий принцип такой защиты – **“разрешить все, что отсутствует в сигнатурных базах”**.

С быстрым ростом количества вредоносных программ увеличилось и число необходимых проверок. При этом все они происходили локально – то есть на компьютере пользователя. В результате сканирование требовало много времени (как правило, несколько часов) и системных ресурсов.

Антивирусный Сканер Cezurity построен иначе. Сначала с компьютера пользователя собираются необходимые данные – цифровые отпечатки (хэши), другие свойства критических файлов, а также информация о местах операционной системы, которые могут быть подвержены заражению. Данные передаются в облако Cezurity Cloud и там анализируются. Анализу подвергаются не только свойства отдельных объектов, но и взаимосвязи между ними, а также их изменения во времени (для анализа изменений во времени необходимо провести несколько сканирований).

За счет того, что обработка данных происходит не на локальном компьютере, а в облаке, проверки Сканером меньше сказываются на производительности. Перенос анализа в облако позволяет увеличить глубину проверки. Для обнаружения опасности сопоставляется большее число свойств объектов.

В отличие от обычных антивирусов Сканер ищет не вредоносные программы в огромном количестве сохраненной на компьютере информации, а наоборот – проверяет, чтобы все критические файлы и места системы были свободны от заражения. Принцип здесь противоположен – **“обнаружить все, что еще не известно (и, соответственно, еще не проверено)”**.

Такой подход позволяет проверить систему быстро – за несколько минут, и незаметно – не отнимая системные ресурсы. Точность обнаружения активных вредоносных программ при этом будет выше по сравнению с обычными антивирусами. Антивирусам для того, чтобы отнести объект к вредоносным, нужно сначала хотя бы раз встретить его в другом месте, проанализировать и внести в сигнатурную базу. Это требует времени, а уникальная атака может быть не обнаружена никогда. Антивирусный Сканер лишен такого недостатка. Если в облаке (Cezurity Cloud) отсутствует информация о каком-либо критическом объекте системы, он анализируется и, если оказывается заражен, то это обязательно будет обнаружено.

Антивирусный Сканер обнаруживает и удаляет все типы вредоносного ПО, включая вирусы, трояны, шпионские программы, вредоносные расширения браузеров, руткиты. При этом он не предназначен для предотвращения заражения, так как не защищает компьютер в реальном времени (on-access scanning). Регулярные проверки Антивирусным Сканером Cezurity позволяют вовремя заметить и вылечить заражение.

Установка и удаление Сканера

Системные требования

Для корректной работы Сканера компьютер должен удовлетворять следующим требованиям:

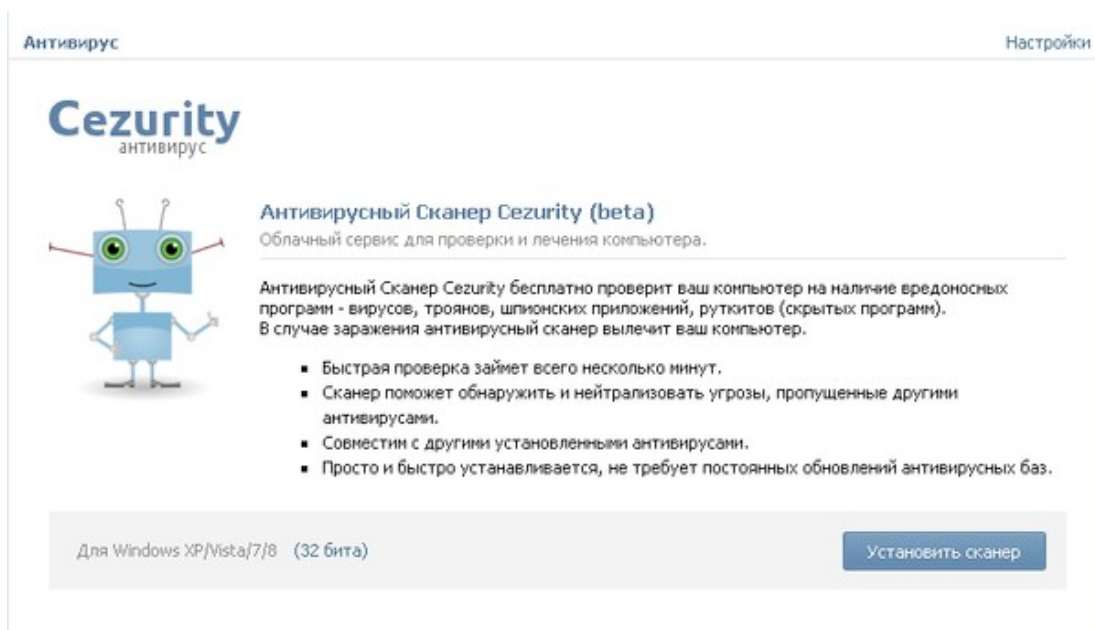
- Операционная система Microsoft: Windows XP SP2 и выше, Windows 2003, Windows 2008, Windows 2012, Windows 7, Windows 8, Windows 8.1.
- Установка и корректная работа Сканера возможна только при наличии подключения к интернету.
- Для установки и запуска Сканера требуются права администратора в системе.

Установка Антивирусного Сканера

Для того, чтобы воспользоваться сервисом, вам нужно установить Сканер на компьютер.

Скачайте дистрибутив программы с официального сайта Cezurity. Для этого зайдите на <http://www.cezurity.com/products/scanner>, кликните на “Скачать и установить”, запустите выполнение программы и следуйте появляющимся инструкциям.


Также Антивирусный Сканер можно установить со страницы соц. сети ВКонтакте. Для этого зайдите на страницу приложения, которая расположена по адресу: <http://vk.com/av>



Антивирус Настройки

Cezurity

антивирус



Антивирусный Сканер Cezurity (beta)

Облачный сервис для проверки и лечения компьютера.

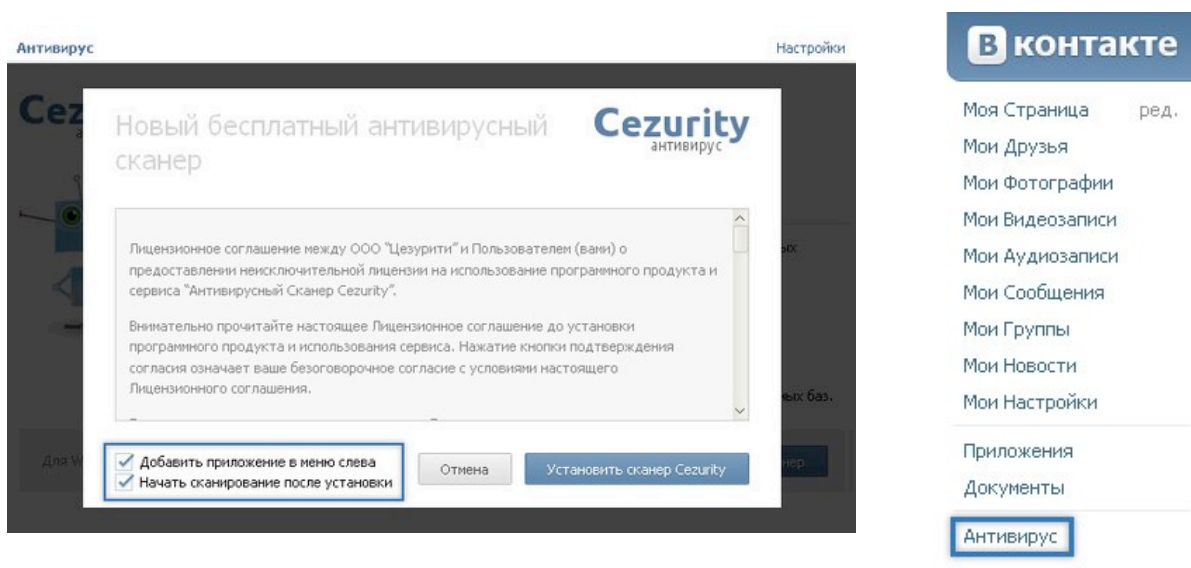
Антивирусный Сканер Cezurity бесплатно проверит ваш компьютер на наличие вредоносных программ - вирусов, троянов, шпионских приложений, руткитов (скрытых программ). В случае заражения антивирусный сканер вылечит ваш компьютер.

- Быстрая проверка займет всего несколько минут.
- Сканер поможет обнаружить и нейтрализовать угрозы, пропущенные другими антивирусами.
- Совместим с другими установленными антивирусами.
- Просто и быстро устанавливается, не требует постоянных обновлений антивирусных баз.

Для Windows XP/Vista/7/8 (32 бита) Установить сканер

Нажмите кнопку “Установить сканер” и следуйте инструкциям.

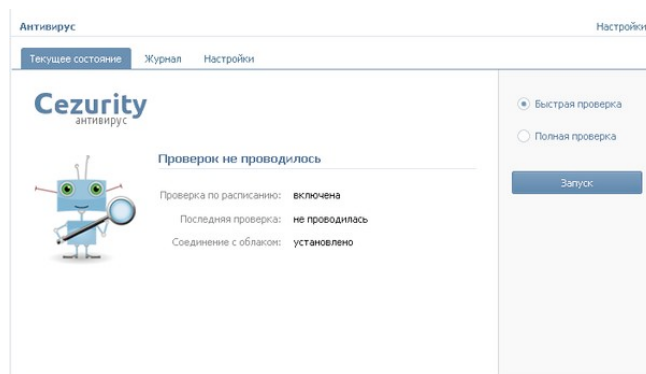
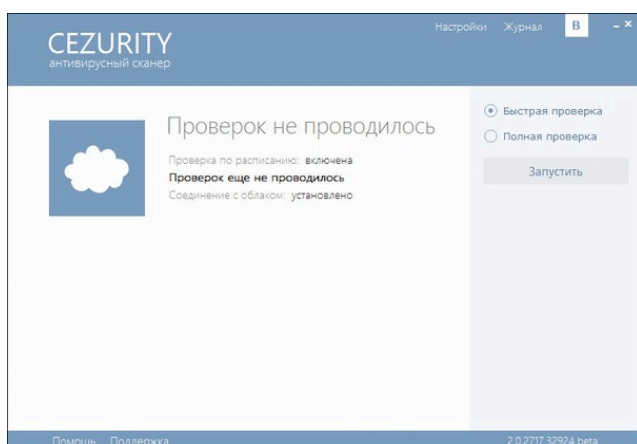
Если вы являетесь пользователем социальной сети ВКонтакте, рекомендуется при установке отметить пункт “Добавить приложение в меню слева”. Это позволит быстро запускать Антивирусный Сканер из окна в социальной сети:



Когда установка будет завершена, значок Сканера появится в области уведомлений (обычно расположена в правом нижнем углу экрана):



Сканер установлен и готов к работе:



Вы можете осуществлять одни и те же действия со Сканером в любом из окон – **в социальной сети** или **на локальном компьютере** – окна автоматически синхронизируются. Управлять Антивирусным Сканером с помощью окна ВКонтакте может быть удобно, когда вы находитесь на странице социальной сети и авторизованы. Учтите, некоторые настройки, доступные в окне Сканера **на локальном компьютере**, отсутствуют в аналогичном окне **в социальной сети**.



Существует два разных дистрибутива Антивирусного Сканера – для 32-битных и 64-битных операционных систем. Разрядность вашей операционной системы определяется автоматически и скачивается дистрибутив для того компьютера, с которого вы зашли на сайт. Если вам нужно скачать дистрибутив для операционной системы с другой разрядностью, выберите соответствующую разрядность вручную.

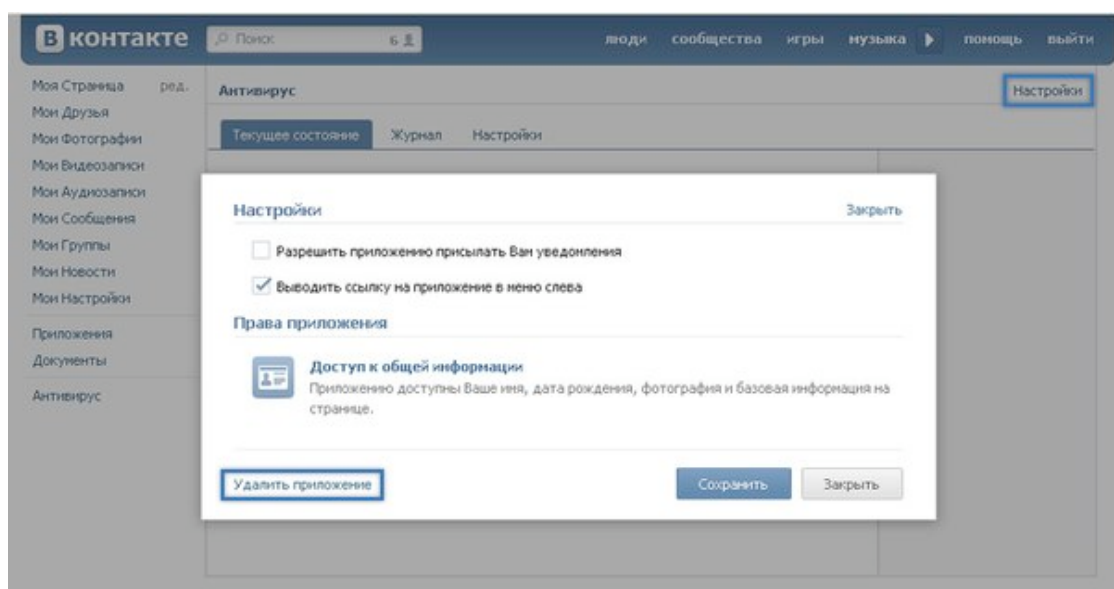
Удаление Сканера

Для удаления Антивирусного Сканера с компьютера выполните следующие действия:

- Нажмите кнопку “Пуск”, выберите пункт “Панель управления”;
- Если у вас Windows XP, зайдите в меню “Установка и удаление программ”;
- Если у вас Windows Vista, Windows 7 или Windows 8, зайдите в меню “Программы и компоненты”;
- В списке программ выберите Cezurity Antivirus Scanner и нажмите кнопку “Удалить”;
- В ответ на предложение удалить программу нажмите кнопку “Да”. Антивирусный Сканер Cezurity будет полностью удален с вашего компьютера.



Удаление Антивирусного Сканера с локального компьютера не приведет к тому, что приложение будет также удалено с вашей страницы ВКонтакте. Для того, чтобы удалить приложение в социальной сети, зайдите в панель настройки приложений на странице Антивирусного Сканера (<http://vk.com/av>) и нажмите “удалить приложение”:



В случае возникновения проблем с удалением, воспользуйтесь утилитой для принудительного удаления: http://www.cezurity.com/temp/remover/Cezurity_Antivirus_Remover.exe



Не используйте для удаления Сканера с компьютера сторонние программы. Антивирусный Сканер обладает средствами самозащиты, которые не позволяют вредоносным программам деактивировать сервис. Использование сторонних программ для удаления Сканера может привести к нестабильной работе операционной системы.

Работа Сканера

Управление Сканером и панель настроек

Вы можете осуществлять одни и те же действия со Сканером в любом из окон – **во ВКонтакте** или **на локальном компьютере** – окна автоматически синхронизируются.

Меню “Настройки” окна **ВКонтакте** позволяет:

- Включить или отключить автоматическую быструю проверку по расписанию и установить режим проверок;
- Настроить действие Сканера при обнаружении опасности. Вы можете выбрать “спрашивать”, либо “действовать автоматически”.

При выборе “спрашивать” Сканер не будет выполнять лечение заражения, а лишь оповестит вас о том, что компьютер заражен.

При выборе “действовать автоматически” Сканер будет:

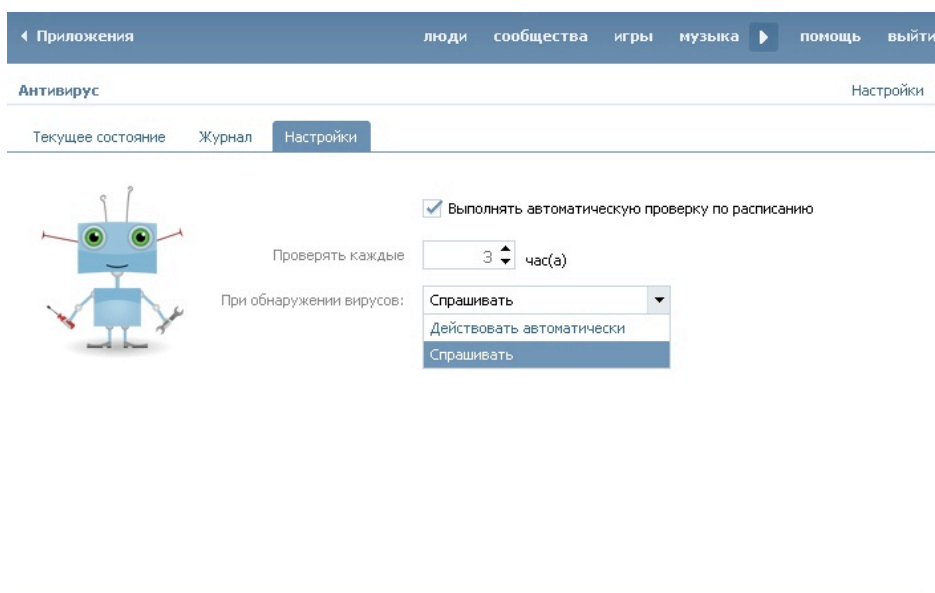
- автоматически удалять угрозы категории “Вредоносная программа (Malware)”, “Нежелательное ПО (Unwanted)”;
- автоматически лечить обнаруженные “Инфицированные файлы (Infected)” – в том случае, если в данный момент существует средство лечения;
- угрозы категории “Потенциально опасное ПО (Riskware)” Сканер автоматически лечить не будет, а только оповестит об их обнаружении. Это сделано для того, чтобы случайно не оказались удалены приложения, которые вы установили самостоятельно, понимая риск их использования.



Если вы все-таки хотите удалить угрозы категории “Потенциально опасное ПО (Riskware)”, убедитесь, что в настройке действия при обнаружении стоит “спрашивать”, после этого запустите быстрое сканирование, а после его окончания удалите угрозы вручную (подробнее об этом см. пункт “Лечение заражений”).

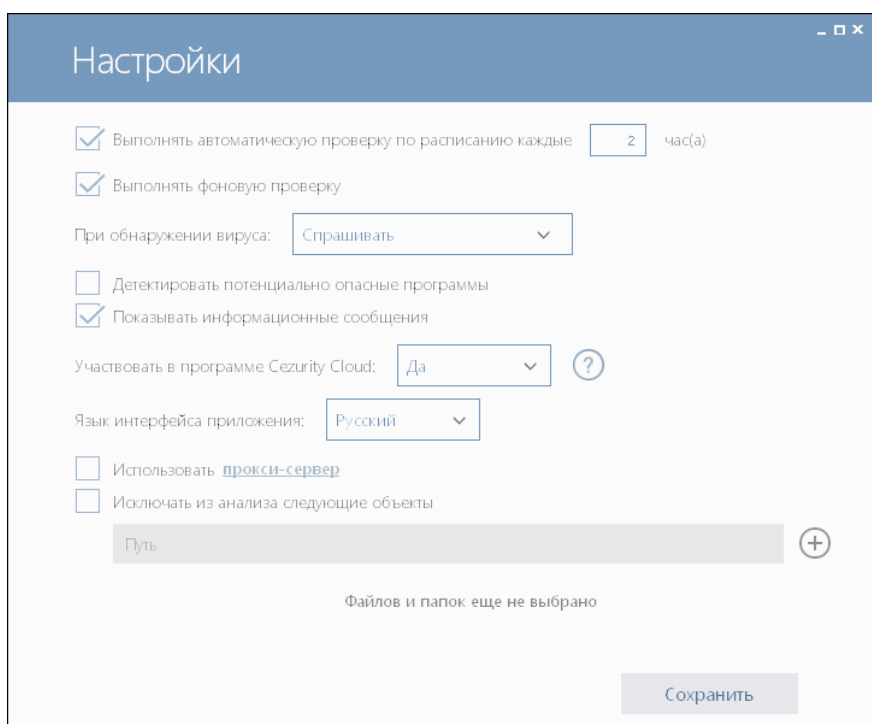


По умолчанию выбрана опция “спрашивать”, то есть Сканер не будет выполнять лечение заражения, а лишь оповестит вас о том, что компьютер заражен.



В окне настроек **на локальном компьютере** можно также:

- Включить или отключить фоновую проверку. Это проверка, которая запускается автоматически, если компьютер не используется. Более подробно про типы проверки см. в разделе “Виды проверок”.
- Включить или отключить детектирование программ, относящихся к категории “Потенциально опасное ПО (riskware)” – за более подробной информацией о степени опасности вредоносных программ обратитесь к разделу “Что может нанести вред компьютеру и данным”.
- Настроить режим оповещений: вы можете отключить некоторые информационные сообщения – например, об обновлении программы. Важные сообщения (например, информацию об обнаруженных угрозах) и сообщения, требующие вашего выбора, отключить нельзя.
- Согласиться или отказаться участвовать в программе Cezurity Cloud. Подробнее об участии в Cezurity Cloud см. в разделе “Участие в программе Cezurity Cloud”.
- Выбрать язык интерфейса Сканера.
- Включить и настроить использование прокси-сервера.
- Настроить список исключений. Если вы включите определенные файлы и папки в список исключений, они не будут анализироваться Сканером.



Список исключений можно использовать, например, в том случае, если на компьютере установлена программа, которая детектируется как опасная, но вы уверены в том, что для вас никакого вреда она не несет.



Если какие-то области находятся в списке исключений, то в ходе проверки отображается, будто они сканируются. На самом деле проверка не происходит.

Участие в программе Cezurity Cloud

Cezurity Cloud – это облачная технология антивирусного анализа, лежащая в основе работы Антивирусного Сканера. Вы можете самостоятельно выбрать степень, в которой ваш компьютер будет обмениваться информацией с Cezurity Cloud.

Для обнаружения опасности Сканер собирает с вашего компьютера необходимую информацию (цифровые отпечатки, свойства критических объектов и мест операционной системы) и передает ее для анализа в облако – в Cezurity Cloud. Несколько уровней участия в Cezurity Cloud главным образом обусловлены разными требованиями к интернет-соединению. На панели настроек вы можете самостоятельно выбрать степень, в которой ваш компьютер будет обмениваться информацией с сервером Cezurity.

Вам нужно выбрать один из трех типов участия в Cezurity Cloud:

- Да (Участвовать) – может передаваться расширенный набор информации о файлах, а также, в случае необходимости, сами тела файлов.
- Частично – передается расширенный набор информации о файлах. Тела файлов передаваться не могут.
- Нет (Отказаться от участия) – на сервер Cezurity передается минимально необходимый для детектирования набор информации о файлах, тела файлов передаваться не могут.

Сбор, обработка и хранение персональных данных пользователя не производится ни для какого из уровней участия в программе Cezurity Cloud. Передаваемые данные не содержат никакой информации, утечки которой можно было бы опасаться. Так, во всех случаях передаются и анализируются только исполняемые файлы, либо информация о них. Пользовательские файлы (документы, например) не передаются и не анализируются.



Вы можете ограничить передачу информации в облако (Cezurity Cloud), включив файл или папку в список исключений – это можно сделать на панели настроек окна приложения **на локальном компьютере**. Никакая информация о файлах и папках, ни сами эти объекты, в этом случае на сервер Cezurity передаваться не будут. Участие в Cezurity Cloud увеличивает точность детектирования вредоносных программ. Более подробную информацию о технологии работы Антивирусного Сканера Cezurity вы можете найти в разделе “Описание Антивирусного Сканера Cezurity”.



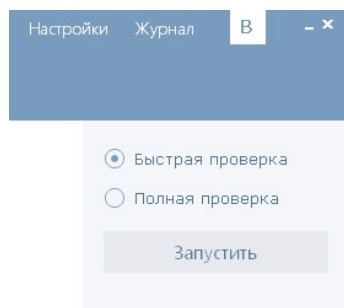
Если вы откажетесь от участия в Cezurity Cloud, информация о критических файлах будет передаваться в облако в ограниченном объеме и, соответственно, эти файлы не смогут быть проанализированы. Так как файлы не будут проанализированы, существует вероятность, что окажется невозможным сделать вывод, являются ли они безопасными. То есть, в этом случае Сканер не всегда может вынести однозначный вердикт об отсутствии или наличии заражения.

Типы проверки компьютера

Сканер осуществляет три типа проверок: быстрое, полное и фоновое сканирование. Быстрое длится несколько минут, полное может занять существенно больше времени – в зависимости от числа установленных программ, объема данных на компьютере и других параметров. Фоновое сканирование запускается автоматически, если компьютер не используется. Быстрое сканирование можно запустить вручную, либо в настройках программы задать расписание – периоды времени, через которые быстрое сканирование будет запускаться автоматически. Полное сканирование можно запустить только вручную. Фоновое сканирование можно включить или отключить на панели настроек.

Для ручного запуска быстрого или полного сканирования компьютера выберите тип проверки и нажмите кнопку “запустить”:

В результате быстрого сканирования проверяются активные процессы, загруженные модули и автозапуск.



Полное сканирование, кроме этого, проверяет все установленные приложения, системный каталог Windows, корневые директории дисков, временные каталоги и еще несколько мест, которые часто используют вредоносные программы для своего распространения и хранения.

Фоновое сканирование представляет собой поэтапную проверку небольшими блоками подверженных заражению областей операционной системы и не является ни быстрой, ни полной проверкой. В частности, фоновое сканирование позволяет обнаружить вредоносные программы, которые либо не запускаются, либо запускаются редко.



Расписание проверок можно установить самостоятельно на панели настроек.



Регулярные проверки позволяют снизить возможный ущерб от заражения – вы можете вовремя увидеть, что компьютер заражен и провести лечение. Также вы можете вовремя предпринять какие-то меры, если в результате заражения были скомпрометированы критичные данные – например, поменять пароли к почте и к другим сервисам.

Результаты проверок

В главном окне Сканера сообщается о результатах последней проверки, либо о тех или иных проблемах в работе сервиса.



Компьютер чист. Все критические файлы вашего компьютера были проанализированы в Cezurity Cloud и являются не просто проверенными, но и доверенными – то есть, они гарантированно не заражены. Ваш компьютер не заражен.



Заражение не обнаружено. Все проверенные файлы не заражены, но не все файлы в данный момент полностью проанализированы и являются доверенными. Вы можете повторить проверку через некоторое время – возможно, к этому моменту все файлы получат статус доверенных. Учтите, так как файлы постоянно анализируются в Cezurity Cloud, при следующем сканировании данный статус может измениться как на “компьютер чист”, так и на “обнаружена опасность”.



Отключена проверка по расписанию. Сообщение означает, что вы отключили регулярные проверки компьютера по расписанию.



Облако недоступно. Данное сообщение означает, что по какой-то причине отсутствует связь с сервером Cezurity и, соответственно, корректная работа Антивирусного Сканера невозможна. Существует несколько возможных причин отсутствия связи с облаком. Наиболее распространены следующие:

- Отсутствует подключение к интернету. В этом случае вам нужно проверить настройки подключения к интернету.
- Работа Антивирусного Сканера блокируется файрволом (брандмауэром). Вам нужно добавить Антивирусный Сканер Cezurity в список программ, которым разрешен доступ в интернет.
- Соединение еще не успело установиться. В некоторых случаях для того, чтобы установилось соединение, может потребоваться какое-то время – обычно это несколько минут. Вам нужно подождать, пока установится соединение. Когда соединение будет установлено, Антивирусный Сканер продолжит работу автоматически.

Вы можете вручную запустить попытку соединиться с облаком. Для этого кликните по оранжевому значку статуса.

Если Антивирусному Сканеру так и не удалось соединиться с сервером Cezurity, воспользуйтесь технической поддержкой (см. пункт “Контактная информация и техническая поддержка”).



Обнаружена опасность. Компьютер заражен. Если в настройках у вас установлено “При обнаружении вируса: действовать автоматически”, то Антивирусный Сканер самостоятельно выберет действие, необходимое для устранения угрозы. Если в настройках Сканера установлено “спрашивать” – вам необходимо вручную выбрать нужное действие: “удалить” (“лечить” для Инфицированных файлов), “пропустить” или “в список исключений” и нажать “Выполнить”. Подробнее о типах действий см. пункт “Лечение заражений”.



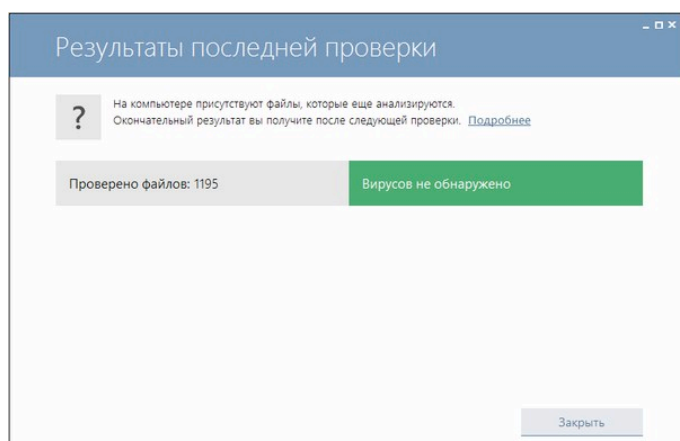
При открытии окна Сканера отображается результат последней проверки.



Иногда для лечения необходимо перезагрузить компьютер. В этом случае Сканер предложит вам выбор – перезагрузить компьютер немедленно или позже. Если вы решите перезагрузить компьютер позже, лечение будет выполнено после перезагрузки.



Если в результатах последней проверки вы видите сообщение с вопросительным знаком в серой иконке, то ваш компьютер проверен не до конца – некоторые файлы еще анализируются в облаке Cezurity. Данный результат будет уточнен после следующей проверки. Рекомендуется запустить быструю проверку через некоторое время.



Лечение заражений

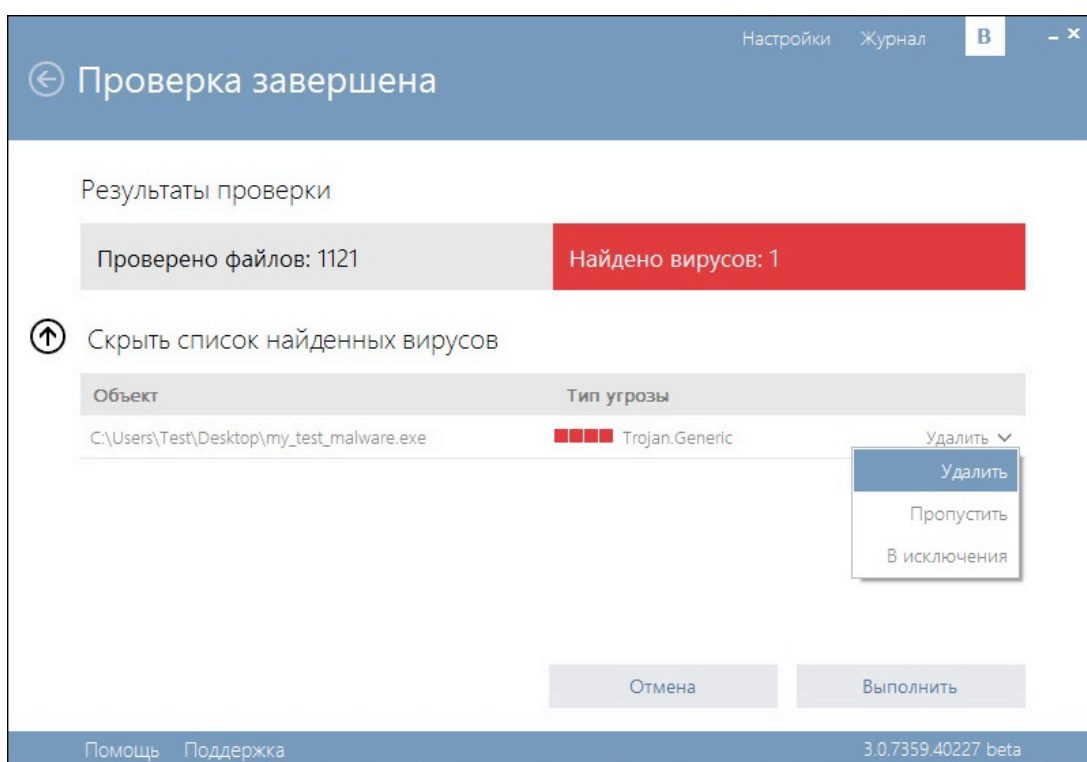
Если в результате проверки на компьютере обнаружена опасность, рекомендуется немедленно провести лечение.

Лечение может проводиться автоматически (то есть без вашего участия) или запускаться вручную. Настроить действие Сканера при обнаружении заражения можно на панели настроек – для этого перейдите в панель настроек и выберите нужное действие при обнаружении вредоносной программы. Это может быть либо “действовать автоматически”, что приведет к автоматическому лечению при обнаружении, либо “спрашивать” – в этом случае Сканер просто оповестит вас о том, что обнаружена опасность.



По умолчанию в настройках установлено “спрашивать”. То есть, Сканер не будет автоматически выполнять лечение, а лишь оповестит вас о том, что компьютер заражен.

Если у вас стоит настройка “спрашивать”, то вам каждый раз самостоятельно нужно будет принимать решение о том, проводить ли лечение. После окончания сканирования, в ходе которого было найдено заражение, Сканер предложит выбор: удалить опасность, пропустить или внести опасный объект в список исключений:



После выбора необходимого действия, для его выполнения нажмите кнопку “выполнить”.



Если вы отказались от удаления заражения, выбрав “пропустить”, для лечения компьютера вам нужно будет снова запустить проверку и дождаться ее окончания.



Если Сканеру не удалось вылечить заражение, рекомендуем вам запустить сканирование и лечение через несколько часов.

Если в настройках выбрана опция “действовать автоматически” Сканер будет:

- автоматически удалять угрозы категории “Вредоносная программа (Malware)”, “Нежелательное ПО (Unwanted)”;
- автоматически лечить обнаруженные “Инфицированные файлы (Infected)” – в том случае, если в данный момент существует средство лечения;

- угрозы категории “Потенциально опасное ПО (Riskware)” Сканер автоматически лечить не будет, а только оповестит об их обнаружении. Это сделано для того, чтобы случайно не оказались удалены приложения, которые вы установили самостоятельно, понимая риск их использования.



Если вы изменили в настройку по умолчанию (“спрашивать”) на “действовать автоматически”, то для удаления “Потенциально опасного ПО (Riskware)” вам придется:

- На панели настроек программы установить действие при обнаружении “спрашивать”;
- Запустить быструю проверку;
- После окончания проверки вручную удалить обнаруженное потенциально опасное ПО (Riskware).

После выполнения лечения Сканер автоматически запустит новое сканирование – это позволит убедиться, что опасность удалена.

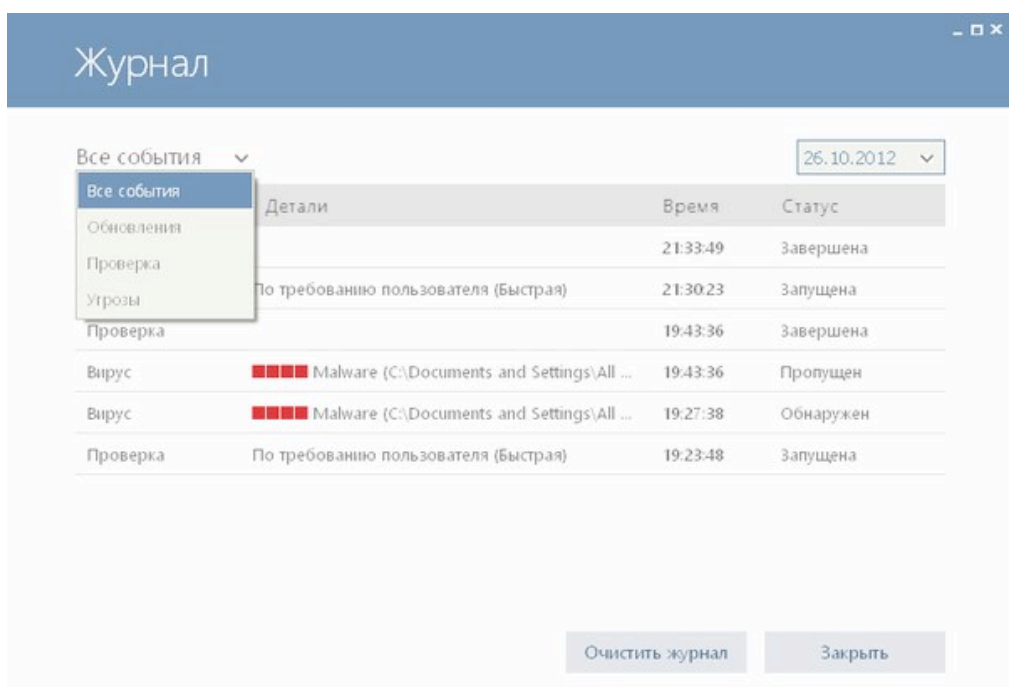
Журнал событий

В Журнале событий фиксируются такие события, как:

- обновления компонентов Сканера
- проведенные проверки
- обнаруженные угрозы
- лечение

Для просмотра Журнала событий кликните “Журнал” в главном окне программы.

При просмотре журнала можно воспользоваться фильтрами:



Фильтры могут быть удобны, если вас интересует какое-то определенное событие – например, информация об обнаруженных угрозах.



В Журнале, открытом **на локальном компьютере**, в таблице отображаются события только за один выбранный день. Для просмотра событий за другие дни необходимо выбрать интересующую дату в выпадающем списке, расположенном сверху справа от таблицы событий.



Журнал событий в окне **в социальной сети** отображает не все события, а только информацию об обнаруженной опасности. Для просмотра всех событий вам нужно открыть журнал в окне приложения **на локальном компьютере**.

Часто задаваемые вопросы (FAQ)

1. Для чего нужен Антивирусный Сканер?

Антивирусный Сканер проверит ваш компьютер и, если он заражен, вылечит.

2. Какие типы вредоносных программ может обнаружить Антивирусный Сканер Cezurity?

Антивирусный Сканер Cezurity обнаруживает все типы вредоносных программ, включая вирусы, трояны, руткиты, шпионские программы, вредоносные расширения браузеров.

3. Сказывается ли работа Антивирусного Сканера на производительности компьютера?

В неактивном состоянии (то есть, когда сканирование не запущено) установленный Антивирусный Сканер не влияет на производительность компьютера. Быстрое сканирование потребляет незначительное количество системных ресурсов и не заметно при обычной работе. Полное сканирование может незначительно замедлять работу компьютера.

4. Сколько времени займет проверка компьютера?

Быстрое сканирование займет около 5 минут. Полное сканирование может продолжаться более часа.

Время сканирования зависит от целого ряда параметров. Это не только объем диска или количество файлов на нем, но также и число запущенных процессов, записей в автозагрузке.

5. У меня на компьютере в папке лежит вредоносная программа. Почему Антивирусный Сканер ее не обнаруживает?

Антивирусный Сканер предназначен для поиска и обезвреживания вредоносных программ, которые уже заразили систему. Такие программы могут, например, перехватывать нажатия клавиш, копировать и отправлять данные, рассылать спам или просто ожидать специального сигнала от своего “командного центра”.

При этом важно помнить, что Антивирусный Сканер проверяет не все, а лишь подвергающиеся заражению области. Например, Антивирусный Сканер не обнаружит вредоносную программу, которая не запущена, на нее нет ссылок из автозапуска, и она при этом не находится в критическом месте системы (например, в системном каталоге).

Это означает, что если на жестком диске в пользовательской директории вы сами просто сохранили (не запуская) вредоносную программу, Антивирусный Сканер ее не обнаружит. Такая программа не может причинить какого-либо вреда, пока вы не запустите ее самостоятельно.

6. Что именно проверяет Антивирусный Сканер Cezurity? Чем отличается быстрое сканирование от полного?

Антивирусный Сканер осуществляет три типа проверок. Это быстрое, полное и фоновое сканирование. Быстрое сканирование может запускаться автоматически по расписанию или вручную, полное сканирование можно запустить только вручную. Фоновое запускается автоматически, если компьютер не используется.

Быстрое сканирование проверяет активные процессы, загруженные модули и автозапуск. Полное сканирование кроме этого проверяет все установленные приложения, системный каталог Windows, корневые директории дисков, временные каталоги и еще несколько мест, которые часто используют вирусы для своего распространения и хранения.

Подробнее о типах сканирования см. пункт “Типы проверки компьютера”.

7. Зависит ли точность обнаружения вредоносных программ от того, как долго Сканер установлен на компьютере?

Да, может зависеть. Во-первых, вынесение окончательных вердиктов о том, являются ли все критические объекты системы доверенными, может занимать некоторое время. При этом важно понимать, что на работающем компьютере такие критические объекты постоянно появляются и изменяются. Во-вторых, в Антивирусном Сканере используется разработанная Cezurity технология динамического обнаружения вредоносных программ. В основе этого способа обнаружения вредоносных программ лежит мониторинг изменений **во времени** критических областей системы и анализ появившихся аномалий. Результаты отдельных сканирований компьютера сравниваются между собой. Таким образом, чем чаще проводится сканирование, тем выше достоверность результатов проверки.

Динамическое обнаружение имеет ряд преимуществ перед технологиями, лежащими в основе других решений. Например, так можно обнаруживать еще не известные антивирусным компаниям вредоносные программы и целенаправленные атаки на отдельные компьютеры.

8. Как часто требуется сканирование?

Рекомендуемая частота проверок зависит от того, как вы используете Антивирусный Сканер.

Можно создать собственное расписание для быстрых проверок. Если на вашем компьютере установлен антивирус, защищающий в реальном времени (антивирусный монитор), мы рекомендуем запускать проверку раз в неделю.

Если же на компьютере нет постоянной защиты в реальном времени (антивирусного монитора), рекомендуется запускать быстрое сканирование как можно чаще – оно незначительно сказывается на производительности компьютера и, скорее всего, вообще не будет вам заметно. По умолчанию Антивирусный Сканер выполняет быстрое сканирование через каждые два часа активной работы компьютера. Это расписание можно изменить в настройках.

Полную проверку нужно запускать самостоятельно – например, в том случае, если у вас есть подозрение, что компьютер заражен.

Помните, что даже частые проверки не могут предотвратить заражение, а лишь позволяют вовремя его заметить и вылечить.

9. Требуется ли обновлять Антивирусный Сканер Cezurity?

Антивирусный Сканер Cezurity не требует обновления сигнатурных баз. Это связано с тем, что сам по себе анализ данных происходит "в облаке", сигнатурные базы на локальный компьютер не скачиваются.

Однако, используемые в Антивирусном Сканере технологии постоянно совершенствуются и некоторые компоненты программы могут обновляться. Актуальность установленной у вас версии Антивирусного Скандера проверяется автоматически.

10. Мои файлы куда-то передаются с компьютера?

Антивирусный Сканер передает на сервер цифровые отпечатки (хэши) и другие свойства (атрибуты) критических файлов. В вирусную лабораторию могут быть отправлены подозрительные исполняемые (Portable Executable) файлы – этот тип файлов не содержит какую-либо информацию, утечки которой можно опасаться.

11. У меня на компьютере уже установлен другой антивирус – могу ли я воспользоваться Антивирусным Сканером Cezurity?

Да. Скорее всего, Антивирусный Сканер Cezurity не будет конфликтовать с работающим антивирусом. Но скорость работы компьютера во время проверки может значительно снизиться, так как сторонний антивирус может перепроверять все файлы, которые смотрит Антивирусный Сканер.

12. У меня на компьютере уже есть другой антивирус. Зачем мне пользоваться Антивирусным Сканером Cezurity?

Во-первых, так можно получить еще одно мнение о том, не заражен ли компьютер. В работе Антивирусного Скандера используются технологии обнаружения, значительно отличающиеся от тех, которые лежат в основе большинства антивирусов. Это позволяет, например, лучше по сравнению с классическими антивирусами детектировать вредоносные программы, скрывающие свое присутствие в системе (руткиты).

Во-вторых, вы можете запускать быстрое сканирование перед тем, как совершить какое-то действие с чувствительными данными – зайти в онлайн-банк, купить что-то через интернет, запустить онлайн-игру и пр.

13. Можно ли проверить Антивирусным Сканером отдельный файл или папку?

Нет. Антивирусный Сканер не проверяет отдельные файлы или папки, а смотрит, не заражена ли система. Проверка отдельных файлов или папок бессмысленна с точки зрения оценки того, заражена ли система (более подробно - см. п. 5).

Если вам нужно проверить отдельный файл, воспользуйтесь сервисом VirusTotal (www.virustotal.com). С помощью VirusTotal можно получить мнение примерно 40 антивирусных компаний о том, чист ли файл от заражения. При этом помните, проверка VirusTotal показывает лишь одно – есть ли данный файл в сигнатурных базах антивирусов. Но вредоносный файл может отсутствовать в сигнатурных базах по той причине, что еще не был обнаружен антивирусной лабораторией ни одной из компаний. К тому же, из отсутствия заражения конкретного файла невозможно сделать вывод о том, что система не заражена.

Если в результате проверки сервисом VirusTotal какого-либо файла с вашего компьютера была обнаружена опасность, настоятельно рекомендуем проверить систему Антивирусным Сканером. Достаточно высока вероятность того, что компьютер заражен.

14. Сколько стоит проверка компьютера и лечение?

Бесплатно.

Контактная информация и техническая поддержка

Антивирусный Сканер разработан и поддерживается компанией Cezurity.

Россия, Санкт-Петербург
ул. Матроса Железняка, 57
+7 (812) 640 4143
office@cezurity.com

Для получения технической поддержки вы можете написать по почте antivirus@cezurity.com, либо задать вопрос в специальной группе Cezurity в социальной сети ВКонтакте: <http://vk.com/cezurity>.

Примечание

Для использования Антивирусного Сканера вам нужно принять условия лицензионного соглашения. Ознакомиться с этими условиями можно при установке Сканера.

Cezurity ©, 2014

