РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

продуктов

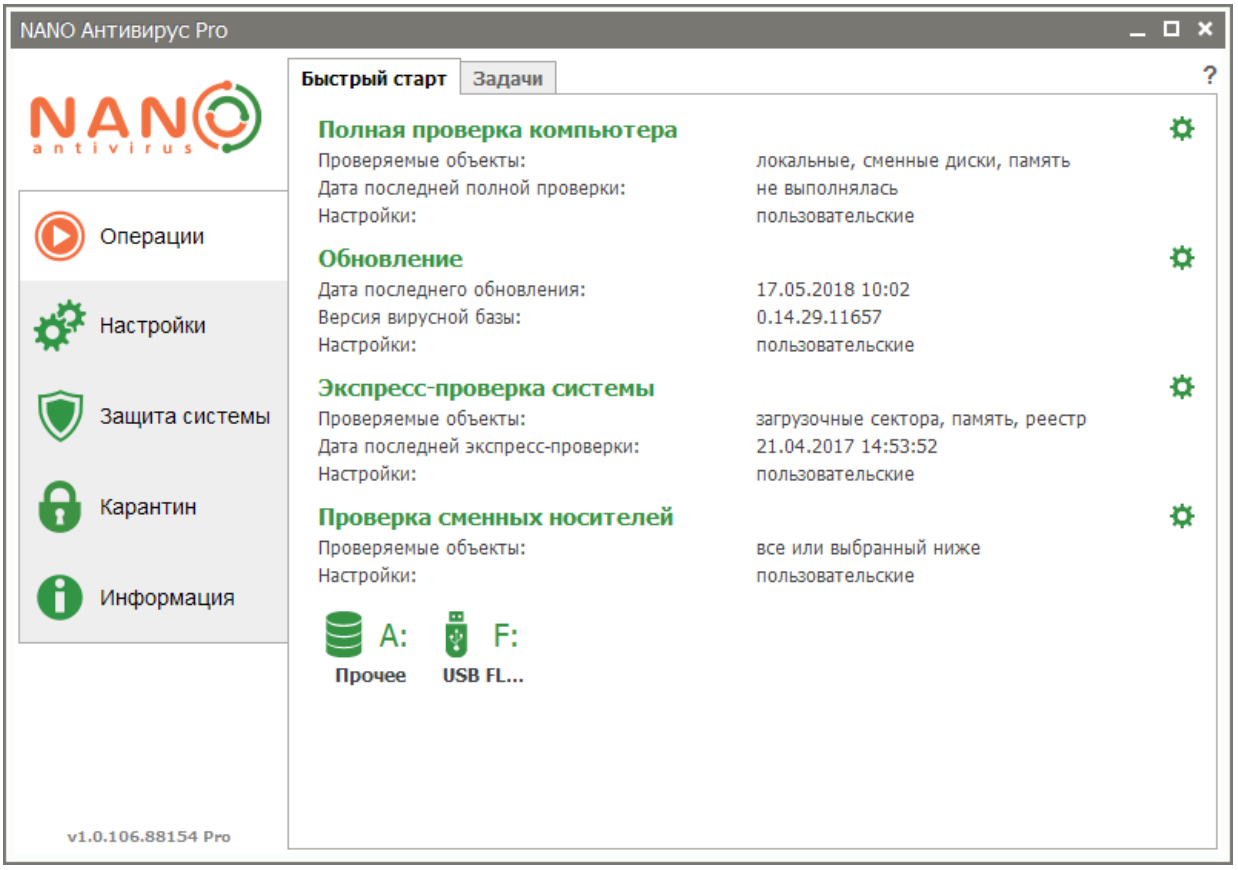
NANO Антивирус PRO и

NANO Антивирус

Оглавление

Что такое NANO Антивирус Pro?

NANO Антивирус Pro – это современное эффективное средство для защиты компьютера от всех видов вирусов, троянских программ (бинарные, макро, скрипт), червей и прочего вредоносного программного обеспечения.



При создании антивирусного комплекса использовались современные собственные разработки в области защиты. Это позволило создать продукт, работающий быстрее большинства аналогичных программ и обеспечивающий при этом высокую надежность в обнаружении любых видов вредоносных программ. Технологии глубокой эмуляции позволяют уверенно находить сложные шифрованные и полиморфные вирусы, не всегда надежно определяемые прочими решениями. Реализована мощная поддержка средств распаковки и работы с архивами, позволяющая выявлять вредоносные объекты, обработанные различными упаковщиками (архиваторами), тем самым обеспечивая защиту от повторных эпидемий, вызванных одними и теми же перепакованными объектами.

Наш продукт удобен в использовании. Механизм оптимизации использования ресурсов системы обеспечивает комфортную работу пользователя с другими приложениями в процессе антивирусной проверки. Предусмотрена возможность использования игрового режима. Удобно организован доступ к выполнению наиболее частых задач. Произведя минимальное количество действий, вы можете выполнить полную проверку компьютера, любого сменного носителя, запустить экспресс-проверку (т.е. проверку только потенциально опасных областей), обновить компоненты антивирусного комплекса.

При необходимости вы можете создавать задачи, выполняемые периодически по установленному вами расписанию, что позволяет автоматизировать большинство действий по обеспечению защиты.

В NANO Антивирус Pro встроена функция защиты системы, которая необходима для обеспечения безопасности вашего компьютера в режиме реального времени. При работе на компьютере с включенной защитой системы все файлы, к которым осуществляется доступ (пользователем или системой), немедленно проверяются на предмет наличия вредоносного ПО.

Сканер веб-трафика мгновенно проверяет все загружаемые из интернета файлы на предмет их возможной вредоносности, а также посещаемые вами сайты на наличие вредоносного кода, что дополнительно защищает ваш компьютер от инфицирования.

Предусмотрена возможность организации доверенной зоны, представляющей собой набор объектов, выбранных пользователем и внесенных в особый список, содержимое которого не подлежит проверке при сканировании. Это позволяет исключить из проверки объекты, в безопасности которых вы уверены, тем самым оптимизируя, например, обработку архивов больших объемов.

Наличие функции карантина позволяет обеспечивать надежную изоляцию выявленных подозрительных объектов. Добавленные в карантин файлы вы можете оперативно направить в нашу службу технической поддержки для дальнейшего анализа.

В NANO Антивирусе Pro встроен ряд функций для большего удобства интеграции комплекса в существующую программную инфраструктуру предприятия и его дальнейшего обслуживания. Возможность зеркалирования и настройки источника обновлений поможет автоматизировать процесс регулярного обновления комплекса в корпоративных сетях. Предусмотрена функция запуска от имени другого пользователя, а также защита паролем настроек комплекса от изменения. Есть возможность автоматизировать действия

антивируса при обнаружении различных видов угроз. Ряд наиболее распространенных операций может выполняться с помощью командной строки.

Программа имеет удобный понятный интерфейс. Доступны несколько тем оформления, позволяющие разнообразить внешний вид NANO Антивируса Pro. Есть возможность использовать как русский язык интерфейса, так и английский.

Часто задаваемые вопросы и ответы на них

Актуальная версия часто задаваемых вопросов и ответов опубликована на нашем сайте.

Справочная система антивирусной программы

Получить доступ к справке можно несколькими способами:

Из контекстного меню: Щелкните правой кнопкой мыши по значку в области уведомлений панели задач. В открывшемся контекстном меню выберите пункт «Помощь».

Из любого активного окна: Нажмите клавишу F1.

Из основных окон антивируса: Щелкните по знаку вопроса в правом верхнем углу окна.

Из окна сканирования: Нажмите кнопку «Справка» в правой нижней части окна.

Установка антивируса на ПК, получение и последующее продление лицензии

Онлайн-установка

Для онлайн-установки скачайте на нашем сайте и запустите файл онлайн-установщика. Далее следуйте указаниям мастера установки. Необходимо подключение к Интернету.

Офлайн-установка

В случае если ваш ПК не подключен к сети Интернет, вы можете установить NANO Антивирус Pro в офлайн-режиме. Для установки NANO Антивируса PRO на компьютер, не имеющий подключения к сети Интернет, необходимо предварительно получить файл лицензии. Файл лицензии вы можете получить по электронной почте через службу поддержки. Для этого вам необходимо отправить на адрес support@nanoav.ru запрос на получение лицензии для офлайн-активации. В письме следует указать, на каком количестве ПК вы планируете использовать эту лицензию, имя и email-адрес, на которые будет выдана лицензия, а также приложить (указать) ключ активации.

Далее скачайте версию для офлайн-установки на нашем сайте. Распакуйте архив, содержащий файлы офлайн-установщика NANO Антивируса Pro. Запустите файл setup.exe. Далее следуйте указаниям мастера установки.

Получение и продление лицензии

В процессе установки вам потребуется активировать вашу лицензию для дальнейшего использования NANO Антивируса Pro. Для получения и продления лицензии вы должны указать свое имя и e-mail. Это необходимо для дальнейшей идентификации вашей копии NANO Антивируса Pro при оказании технической поддержки и т.д. При необходимости введите настройки для прокси-сервера. Подробнее о настройках сети – в разделе Сеть.

После заполнения необходимых полей нажмите кнопку **Получить**.

Получить лицензию онлайн

> Если у вас нет файла лицензии, вы можете немедленно активировать антивирус в режиме онлайн. Требуется подключение к сети Интернет.

Ключ активации

> Если у вас есть ключ, введите его для активации версии NANO Антивируса Pro, которая соответствует данному ключу.

Профессиональная пробная

> Выберите эту опцию, если хотите установить NANO Антивирус Pro в пробном 30-дневном режиме. Опция доступна только в NANO Антивирусе Pro.

Подписаться на новости компании

Выберите эту опцию, если хотите получать новости компании на указанный вами при регистрации e-mail.

Загрузить лицензию из файла

Если у вас есть файл лицензии, загрузите его для активации версии NANO Антивируса Pro, которая соответствует данному файлу лицензии.

Срок действия лицензии зависит от типа лицензии и может варьироваться. После завершения срока действия лицензии обновления антивируса станут недоступны. За 7 дней до срока истечения лицензии появится уведомление, напоминающее о необходимости продлить лицензию и предлагающее различные варианты дальнейших действий.

Динамические лицензии

В NANO Антивирусе Pro мы используем принципиально новый — гибкий и удобный тип лицензирования. Теперь вам не нужно заранее решать, для какого количества устройств нужна лицензия сейчас или понадобится в будущем. Мы предоставляем комплекты дней защиты, которыми вы пользуетесь по вашему усмотрению, распределяя их на нужное количество устройств. Более того, при установке на дополнительное устройство вы получаете дополнительные бонусные дни защиты!

Актуальная информация о бонусной системе — на нашем сайте.

Работа с антивирусом

Проверка на наличие вредоносных программ

В антивирусе предусмотрена возможность проведения различных видов проверок. Ниже перечислены доступные типы проверки и описана процедура их выполнения.

Полная проверка

В процессе полной проверки сканируются все области, процессы, файлы и папки вашего ПК. Рекомендуется запустить полную проверку после первой установки антивируса. Также рекомендуется проводить полную проверку после каждого вылеченного активного заражения. Полная проверка может занять продолжительное время.

Экспресс-проверка

При экспресс-проверке сканируются лишь наиболее уязвимые области ПК. Мы рекомендуем проводить проверку перед началом работы на ПК, а также после каждого обновления антивируса. Кроме того, рекомендуется провести проверку при признаках заражения ПК. Вы можете включить автоматическое выполнение экспресс-проверки при запуске антивируса в меню **Настройка**, вкладка **Общие**.

Проверка сменных носителей

В процессе проверки сканируются сменные носители, подключенные к вашему ПК. Во избежание заражения рекомендуется проверять все сменные носители перед началом работы с ними. По умолчанию при подключении сменного носителя появляется запрос на проверку. Вы можете настроить автоматическую проверку сменных носителей в меню **Настройка**, вкладка **Общие**.

Выборочная проверка

При проведении выборочной проверки вы сами выбираете объекты (папки, файлы) и области, которые будут просканированы антивирусом. Вы можете установить дополнительные настройки, с которыми будет проводиться сканирование. Обратите внимание, что количество доступных настроек и их вид зависят от установленной в данный момент темы оформления. Для сканирования одного файла или папки можно также воспользоваться контекстным меню проводника Windows. Щелкните правой кнопкой мыши по папке или файлу, которые вы хотите проверить, и выберите в появившемся контекстном меню пункт **Проверить NANO Антивирусом/NANO Антивирусом Pro**.

Ниже перечислены области ПК, которые можно выбрать для выборочной проверки.

Файлы и папки

При выборе данной области проверки будут просканированы только выбранные вами файлы и папки, расположенные по заданному пути на компьютере

пользователя или в локальной сети. Данный вид проверки удобен для целевой проверки конкретных файлов и папок.

Оперативная память

При выборе данной области проверки будет просканирована вся оперативная память компьютера, включающая все запущенные процессы и служебные данные. Проверка данной области полезна при подозрении на заражение компьютера, которое может выражаться в следующих симптомах: странное поведение ПК, его неустойчивая работа и т.п.

Загрузочные области

При выборе данной области проверки будут просканированы объекты на жестких дисках, отвечающие за загрузку компьютера. Проверка данной области может быть полезна при подозрении на заражение вашего компьютера вредоносным программным обеспечением, запускающимся до загрузки операционной системы.

Рабочий стол

При выборе данной области проверки будут просканированы все объекты, находящиеся на рабочем столе пользователя, а также программы, ярлыки которых находятся на рабочем столе. Проверка бывает полезна, если вы пользуетесь рабочим столом для сохранения документов, загруженных из Интернета, а также в случае, если вы обнаружили на рабочем столе неизвестные ярлыки, ранее там отсутствовавшие.

Документы

При выборе данной области проверки будут просканированы библиотеки. Такой тип сканирования полезен для периодической проверки ваших текущих документов.

Создание задачи сканирования

Вы также можете создать задачу сканирования с собственными настройками. **Внимание!** Количество создаваемых задач может ограничиваться в зависимости от типа вашей лицензии! На вкладке **Задачи** пункта меню **Общие** установите курсор на пункте **Задачи сканирования**. Выберите команду **Добавить задачу сканирования с заданными настройками**. Далее примените к новой задаче необходимые настройки.

Настройки сканирования

В большинстве тем оформления вы можете настроить параметры сканирования. Настройки для основных задач сканирования, а именно для полной проверки,

экспресс-проверки и проверки сменных носителей, доступны на вкладке **Быстрый старт** пункта меню **Общие**. Для настройки пользовательской задачи выделите нужную задачу в дереве задач, затем выберите команду **Настроить выбранную задачу сканирования**. Доступна настройка следующих параметров задачи:

Выбор областей сканирования

За возможность управления этой опцией отвечают следующие настройки:

Системная задача

Внимание! Наличие данной опции зависит от типа вашей лицензии!

> При выборе этой опции задача сканирования будет выполняться для всех пользователей данного ПК. Опция полезна в том случае, если на одном ПК работают несколько пользователей под разными аккаунтами.

Объекты сканирования

> Добавьте те файлы, папки и области сканирования, которые вы хотите проверять в рамках данной задачи.

Фильтрация файлов при сканировании

По умолчанию антивирус сканирует все файлы, вне зависимости от их расширения, типа или размера. Иногда бывает полезно указать конкретные параметры тех файлов, которые вы хотите просканировать. Это может значительно ускорить проверку, но в то же время может снизить уровень обнаружения вредоносных файлов. При применении фильтрации вы должны учитывать этот факт.

За возможность управления этой опцией отвечают следующие настройки:

Сканировать все потенциально опасные расширения

> Используется список расширений, установленный по умолчанию для обеспечения режима оптимальной защиты.

Сканировать файлы с соответствующими расширениями

> Позволяет задать список расширений, который будет использоваться при сканировании. Вы можете как добавлять, так и удалять нужные значения.

Сканировать файловые потоки

Позволяет сканировать служебные атрибуты файлов, которые доступны на некоторых файловых системах. Иногда такие атрибуты используются вредоносной программой для своих целей.

Не проверять объекты размером более N Мб

Позволяет установить размер проверяемого объекта. В некоторых случаях это бывает полезно для ускорения проверки. При этом следует учитывать, что вредоносная программа может находиться и в файле большого размера.

Глубина вложенности

Позволяет установить ограничения на глубину проверки для архивов. Уменьшение глубины проверки может ускорить процесс сканирования. Однако следует иметь в виду, что вредоносная программа может находиться на достаточно глубоком уровне вложенности.

Режим проверки защищенных объектов

Позволяет задать реакцию антивируса при проверке объекта, защищенного паролем. Как правило, это могут быть архивы, защищенные паролем. Антивирус может в данном случае интерактивно запросить пароль при проверке такого объекта, использовать ранее введенный пароль или пропустить объект.

Действия антивируса при обнаружении опасных объектов

Вы можете настроить действия, которые будут выполняться антивирусом при обнаружении вредоносных, подозрительных или потенциально опасных объектов. Для этого выберите желаемое действие для каждого типа объекта. Также вы можете включить опцию сохранения исходных резервной копии для всех изменяемых (удаляемых или вылеченных) файлов в специальное защищенное хранилище. Это может быть полезно, например, в случае ложного срабатывания на файле.

Выполнение по расписанию

Вы можете установить удобное для вас расписание, по которому будет выполняться задача сканирования.

Дополнительные настройки

Список дополнительных настроек может варьироваться в зависимости от установленной в данный момент темы оформления.

Оптимизация использования процессора

Эта опция полезна в том случае, если антивирус установлен на ПК с многоядерным процессором. В этом случае оптимизация использования процессора позволяет проводить сканирование, равномерно распределяя нагрузку, что ускоряет процесс проверки.

Не показывать окно при старте задачи

При включении данной опции окно сканирования не будет выводиться при старте задачи. Данная опция удобна в том случае, если вы хотите чтобы задача запускалась в фоновом режиме, не отвлекая от работы на ПК.

Не выводить сообщения об ошибках

Данная опция позволяет отключить выведение в окне сканирования информации об возможных ошибках, произошедших в процессе проверки некоторых файлов.

Показать окно при завершении задачи

При включении данной опции, после завершения задачи будет активизировано окно сканирования. Данная опция удобна, если по окончании сканирования вы хотите просмотреть подробную информацию о результатах проверки.

Выводить сообщения об архивах, защищенных паролем

Данная опция активизирует вывод в окно сканирования информации об обнаруженных архивах, защищенных паролем.

Не запускать задачу при работе от батареи

Данная опция предназначена для ноутбуков. Она полезна для экономии заряда батареи в случае, если ноутбук в момент времени старта задачи не подключен к сети.

Процесс сканирования

После запуска проверки на наличие вредоносного программного обеспечения на экране появляется окно процесса сканирования. Окно содержит общую информацию о задаче сканирования, информацию об объектах, обнаруженных в процессе сканирования, а также элементы управления процессом, позволяющие перевести сканирование в фоновый режим, приостановить или завершить. В процессе сканирования динамически выводится список объектов, обнаруженных в процессе сканирования. В настройках сканирования можно отключить вывод имен объектов, на которых произошли ошибки, а также архивов, защищенных паролем. В этом случае в списке будут отображаться только вредоносные, подозрительные и потенциально опасные объекты. При щелчке на имени

объекта правой кнопкой мыши выводится контекстное меню, дающее возможность произвести над обнаруженным объектом ряд действий, таких как лечение, перенос в карантин и т.п.

Обновление антивируса

Чтобы обеспечить надлежащую защиту вашего ПК, необходимо регулярно обновлять вирусную базу. По умолчанию после установки антивируса создается задача автоматического обновления с оптимальными для большинства пользователей настройками. Вы также можете по своему желанию обновлять антивирус вручную. Обновление вручную доступно из пункта **Операции** главного меню, вкладка **Быстрый старт**. Нажмите на поле **Обновление**. Будут применены текущие настройки обновления.

Вы также можете создать задачу обновления с собственными настройками. **Внимание!** Количество создаваемых задач может ограничиваться в зависимости от типа вашей лицензии!

На вкладке **Задачи** пункта меню **Общие** установите курсор на пункте «Задачи обновления». Выберите команду «Добавить задачу обновления с заданными настройками». Далее примените к новой задаче необходимые настройки. Аналогичным образом вы можете изменить настройки задачи обновления, применяемой по умолчанию.

В большинстве тем оформления вы можете настроить параметры обновления. Для основной задачи обновления настройки доступны на вкладке «Быстрый старт» пункта меню «Общие». Для настройки пользовательской задачи выделите нужную задачу в дереве задач, затем выберите команду «Настроить выбранную задачу обновления». Доступна настройка следующих параметров задачи:

Свойства задачи

Системная задача

Внимание! Наличие данной опции зависит от типа вашей лицензии!

> При выборе этой опции задача обновления будет выполняться для всех пользователей данного ПК. Опция полезна в том случае, если на одном ПК работают несколько пользователей под разными аккаунтами.

Показать окно при завершении задачи

При включении данной опции, после завершения задачи будет активизировано окно обновления. Данная опция удобна, если по окончании обновления вы хотите просмотреть подробную информацию о процессе обновления.

Источник обновления

Данная опция позволяет настроить источник, который будет использоваться для получения обновлений антивируса.

Внимание! Наличие данных опций зависит от типа вашей лицензии! Доступны следующие источники:

Официальный источник обновления

Использование официального сервера обновления удобно в случае, если ПК имеет стабильный неограниченный доступ в Интернет.

Папка

Использование этой опции удобно, если доступ в Интернет лимитирован, неустойчив или отсутствует. В этом случае файлы обновлений можно получать на другом ПК, подключенном к Интернету, и переносить в назначенную папку.

Сервер

Опция предназначена, в первую очередь, для использования в корпоративных сетях. Обновление с пользовательского сервера позволяет оптимизировать использование ресурсов при обновлении большого количества ПК.

Авторизация

Если для доступа к пользовательскому серверу требуется авторизация, введите логин и пароль, которые будут использоваться при доступе к обновлениям.

Зеркалирование

Данная опция удобна для настройки процесса обновления в корпоративной сети. При включении данной опции файлы обновления будут автоматически сохраняться в указанной папке, которую можно установить в качестве источника обновления.

Выполнение по расписанию

Вы можете установить удобное для вас расписание, в соответствии с которым будет выполняться обновление.

Обновлять автоматически

Рекомендуется установка режима «Автоматически», предлагающего оптимальную частоту обновления.

История задач

В антивирусе предусмотрено сохранение подробной информации о выполненных задачах сканирования. Для управления историей задач выберите вкладку **Задачи** пункта главного меню **Операции**. Вы можете просмотреть выполненную задачу, выполнить ее повторно либо удалить из списка.

Активные задачи

Для управления задачами, выполняющимися в текущий момент, выберите вкладку **Задачи** пункта главного меню **Операции**. Далее воспользуйтесь пунктом **Активные задачи**. Кроме того, активные задачи доступны из контекстного меню в области уведомлений.

Дополнительные настройки антивируса

Внимание! Наличие данных опций зависит от типа вашей лицензии!

Защита от изменений настроек

Вы можете защитить настройки антивируса с помощью пароля. Данная опция полезна для случаев, когда необходимо предотвратить несанкционированное изменение важных настроек пользователями. При активизации режима, без ввода пароля будет невозможно отключить защиту системы, изменить настройки сканирования и обновления, удалить или изменить пользовательские задачи и т.п.

Автоматическое включение игрового режима

При включении этой опции игровой режим будет активизироваться при запуске полнооконных приложений. В игровом режиме на экран не выводятся уведомления, а также не воспроизводятся звуковые оповещения.

Не запускать обновление по расписанию

При включении этой опции, в случае если будет активен игровой режим, задачи обновления по расписанию не будут запускаться до выключения игрового режима.

Участие в программе улучшения качества

Мы будем признательны за ваше участие в программе улучшения качества. В случае активирования данной опции мы будем получать анонимную, не

привязанную к конкретному пользователю информацию об ошибках и т.п., которая поможет нам устранять возможные неполадки и улучшать наш продукт.

Вид интерфейса

В антивирусе доступны несколько тем оформления, различающиеся внешним видом и набором функций. Кроме того, вы можете выбрать язык интерфейса.

Информационные сообщения

Вы можете задать местоположение выводимых на экран ПК уведомлений, не требующих действия пользователя. Кроме того, вы можете выбрать подходящий вам режим вывода уведомлений. Возможно установить режим, при котором выводятся все, либо только важные уведомления – об ошибке, произошедшей во время обновления, а также о завершении задачи сканирования, в рамках которой было обнаружено вредоносное ПО.

Уведомлять об устаревших базах

Своевременное обновление вирусных баз необходимо для обеспечения надлежащего уровня защиты. Включите уведомление для того чтобы не пропустить момент, когда базы будут нуждаться в обновлении.

Звуковые оповещения

Вы можете включить или отключить звуковое оповещение о событиях антивируса. Можно выбрать оповещение обо всех событиях либо только об обнаружении вредоносного, потенциально опасного или подозрительного ПО.

Сеть

В случае если вы подключены к сети Интернет через прокси-сервер, добавьте необходимые параметры в настройки сети. Данные настройки будут использоваться для всех действий антивируса, предполагающих работу с сетью, а именно: обновление антивируса, отправка подозрительных файлов для дальнейшего анализа, получение лицензии и т.д. Вы также можете задать максимальный размер подозрительных файлов, отправляемых из папки карантина для дополнительного исследования.

Постоянная защита системы

В антивирус встроена функция постоянной защиты системы, которая отвечает за безопасность вашего компьютера в режиме реального времени. Комплексная защита системы обеспечивается файловой защитой и веб-защитой. При работе на компьютере с включенной файловой защитой все файлы, к которым осуществляется доступ пользователем или системой, немедленно проверяются на наличие вредоносного кода. Веб-защита обеспечивает безопасную работу в

Интернете, инициируя проверку на предмет наличия вредоносного содержимого всех скачиваемых файлов, а также посещаемых сайтов. В случае обнаружения угрозы немедленно появляется оповещение. Вы можете включить или отключить компоненты функции защиты на соответствующих вкладках главного окна. Мы не рекомендуем отключать защиту системы, так как это повысит риск инфицирования вашего ПК. Для защиты системы доступен ряд настроек:

Автоматически запрещать доступ к зараженным файлам

В случае включения этой опции все обнаруженные вредоносные файлы будут немедленно автоматически блокироваться.

Проверять HTTP-трафик

Отключите эту опцию, если вы не хотите, чтобы в процессе работы веб-защиты проверялись посещаемые вами веб-страницы.

Проверять почтовый трафик

Отключите эту опцию, если вы не хотите, чтобы проверялся ваш почтовый трафик.

Проверять FTP-трафик (пассивный режим)

Отключите эту опцию, если вы не хотите, чтобы проверялся FTP-трафик.

Блокировать использование активного режима FTP

Включите опцию для блокировки активного FTP-трафика.

Журнал событий

Информация об угрозах, обнаруженных с помощью файловой и веб-защиты, выводится в журнал защиты системы. Чтобы просмотреть информацию, относящуюся к интересующему вас источнику событий, выберите в выпадающем меню соответствующий пункт.

Значок в области уведомлений и контекстное меню

После установки антивируса в области уведомлений появляется значок программы. Внешний вид значка может изменяться в зависимости от режима работы антивируса и от установленной темы оформления. Текущий статус антивируса подчеркивается анимацией иконки для того, чтобы визуально информировать пользователя о выполняемых задачах либо предупреждать о проблемах. При щелчке правой кнопкой мыши по значку антивируса,

находящемуся в области уведомлений панели задач, открывается контекстное меню. Меню позволяет получить быстрый доступ к ряду функций антивируса:

Открыть NANO Антивирус/NANO Антивирус Pro

Будет открыто главное окно антивируса.

Обновить

Будет выполнена задача обновления, принятая по умолчанию.

Выключить защиту системы

Будет выключена полностью защита системы. Для отключения файловой защиты и веб-защиты по отдельности перейдите в главное окно антивируса, пункт меню **Защита системы**.

Включить защиту системы

Будет выключена полностью защита системы. Для отключения файловой защиты и веб-защиты по отдельности перейдите в главное окно антивируса, пункт меню **Защита системы**.

Включить/выключить игровой режим

Будет включен/выключен специальный режим, ограничивающий действия NANO Антивируса Pro во время работы полноэкранных приложений для большего удобства пользователя.

Сканирование объектов

Быстрый доступ к сканированию любого диска в системе.

Задачи сканирования

Быстрый доступ к старту любой пользовательской задачи сканирования.

Активные задачи

Быстрый доступ к управлению задачами сканирования и обновления, выполняемыми в текущий момент.

Помощь

Переход в справочную систему антивируса.

Выход

> Завершение работы визуальной части антивируса. При этом после завершения работы визуальной части антивирус продолжает защищать ваш ПК, запланированные задачи будут выполняться в установленное время. Для повторного запуска воспользуйтесь пунктом меню: «Пуск->Все программы->NANO Антивирус/NANO Антивирус Pro».

Доверенная зона

Доверенная зона – это набор объектов, выбранных пользователем и внесенных в особый список, содержимое которого не подлежит проверке при сканировании. Существуют различные причины для внесения объекта в доверенную зону. Например, в проверяемой папке хранится архив большого объема, в безопасности которого вы уверены. Для ускорения работы антивируса можно исключать такие объекты из проверки. Также возможен случай, когда вы, осознавая риск, пользуетесь условно-опасной программой, и антивирус воспринимает её как вредоносное программное обеспечение. Внесение такого объекта в доверенную зону поможет решить проблему. Для формирования доверенной зоны перейдите в соответствующее окно. Вы можете добавлять, удалять и редактировать правила для файлов и папок, приложений и веб-адресов.

Карантин

Карантин – это хранилище потенциально опасных объектов, обнаруженных в процессе сканирования, добавленных вручную для дальнейшего анализа, либо хранящихся в виде резервных копий с возможностью последующего восстановления. В карантине доступны дополнительные действия над файлами с помощью контекстного меню, которое вызывается щелчком правой кнопки мыши на списках файлов.

Для карантина доступен ряд настроек:

Действия при обнаружении подозрительного объекта в карантине

Вы можете выбрать действия, которые будут выполняться антивирусом для подозрительных объектов в карантине в момент их добавления или по итогам пересканирования.

Спросить пользователя

В случае если находящийся в карантине объект будет признан подозрительным, появится уведомление с запросом дальнейших действий.

Отправить для анализа

Подозрительный объект будет отправлен в вирусную лабораторию для дополнительного анализа. Требуется подключение к сети Интернет.

Не отправлять

Подозрительный объект на анализ в вирусную лабораторию отправлен не будет, запрос действий по объекту больше не будет выводиться. Вы можете в дальнейшем отправить данный подозрительный объект в вирусную лабораторию самостоятельно, перейдя в меню **Карантин** и воспользовавшись контекстным меню.

Прочие настройки

Пересканировать карантин после каждого обновления

Включите эту опцию, если хотите, чтобы антивирус автоматически перепроверял всей файлы, помещенные в карантин, используя самую свежую вирусную базу.

Автоматически восстанавливать из карантина чистые объекты

Если по итогам пересканирования с обновленной вирусной базой объект будет признан чистым, он будет автоматически удален из карантина и восстановлен в первоначальное месторасположение.

Автоматически лечить инфицированные объекты в карантине

Если по итогам пересканирования с обновленной вирусной базой объект будет признан инфицированным, будет автоматически запущено его лечение.

В случае добавления в карантин вредоносного файла появится запрос о дальнейших действиях над файлом.

Работа в командной строке

В NANO Антивирусе Pro предусмотрена возможность запуска некоторых операций из командной строки. Для получения базовой справки по доступным видам операций наберите в командной строке: nanoavcl --help. Для получения развернутой информации по всем ключам, доступным для интересующей вас конкретной операции, наберите в командной строке: nanoavcl %имя операции% --help.

Уведомления, выводимые антивирусом и работа с ними

В процессе работы антивируса могут появляться различные уведомления. Существуют уведомления двух видов – информационные и интерактивные.

Информационные уведомления сообщают, соответственно, некоторую информацию о процессе работы антивируса и не требуют никаких ответных действий пользователя. Такие уведомления автоматически исчезают с экрана через некоторое время, также их можно закрыть с помощью щелчка правой кнопкой мыши в области уведомления.

Интерактивные уведомления предлагают пользователю произвести определенные действия для продолжения работы программы.

Работа с интерактивными уведомлениями

Интерактивные уведомления могут появляться при обнаружении угрозы во время сканирования, в процессе работы постоянной защиты системы, при необходимости обновления антивируса, перезапуска антивируса и в ряде других ситуаций, когда для продолжения работы необходим выбор пользователем дальнейшего действия.

Для уведомлений об угрозах доступны следующие действия:

Лечить

Будет предпринята попытка лечения обнаруженного вредоносного файла. Резервная исходная копия файла будет сохранена в защищенное хранилище карантина с возможностью последующего восстановления при необходимости.

Лечить все

К каждому вредоносному файлу, обнаруженному в рамках текущего сканирования, будет предпринята попытка лечения. Резервные исходные копии файлов будут сохранены в защищенное хранилище карантина с возможностью последующего восстановления при необходимости.

Удалить

Обнаруженный вредоносный файл будет удален. Резервная исходная копия файла будет сохранена в защищенное хранилище карантина с возможностью последующего восстановления при необходимости.

Удалить все

Все вредоносные файлы, обнаруженные в рамках текущего сканирования, будет удалены. Резервные исходные копии файлов будут сохранены в защищенное хранилище карантина с возможностью последующего восстановления при необходимости.

Блокировать

Вредоносный файл, к которому обратилась система, будет разово заблокирован для этого обращения.

Блокировать все

Вредоносный файл, к которому обратилась система, будет заблокирован для этого и дальнейших обращений. Запрет будет действовать до момента перезапуска антивируса. Настройка действий над обнаруженными с помощью защиты системы инфицированными файлами будет изменена на «Блокировать».

Отложить

Обнаруженный во время сканирования вредоносный файл будет пропущен без обработки. Вы можете позднее применить к нему нужные действия, воспользовавшись контекстным меню в окне сканирования.

Отложить все

Все обнаруженные во время сканирования вредоносные файлы будут пропущены без обработки. Вы можете позднее применить к обнаруженным файлам нужные действия, воспользовавшись контекстным меню в окне сканирования.

Разрешить доступ

Разовый доступ к обнаруженному вредоносному файлу будет разрешен.

Добавить в доверенную зону

Данный файл будет добавлен в доверенную зону.

Пометить как ложное срабатывание

Если вы уверены в безопасности файла, детектируемого антивирусом как вредоносный, пометьте его как ложное срабатывание. отправьте его нам для анализа ситуации.

Изолировать

Обнаруженный подозрительный файл будет перемещен в карантин.

Изолировать все

> Все подозрительные файлы, обнаруженные в рамках текущего сканирования, будет перемещены в карантин.

При сканировании защищенных архивов будет появляться уведомление с запросом пароля в случае, если такая настройка была добавлена для задачи сканирования. Для продолжения работы введите пароль в соответствующее поле.

Применить для всех подобных объектов

> При выборе этой опции введенный пароль будет применен для всех защищенных паролем архивов, обнаруженных в рамках текущей задачи сканирования.

При подключении сменного носителя к ПК появится уведомление с запросом дальнейших действий в случае если в общих настройках была выбрана соответствующая установка. Выберите действие, которое вы хотите применить к сменному носителю.

Всегда выполнять выбранное действие

> При выборе этой опции примененное действие будет выполняться каждый раз при подключении сменного носителя.

Удаление антивируса

Чтобы удалить антивирус с компьютера, выберите команду Удалить NANO Антивирус/NANO Антивирус Pro (меню Пуск>Все программы>NANO Антивирус/NANO Антивирус Pro). Далее следуйте указаниям программы удаления.

Техническая поддержка

Специалисты нашей службы технической поддержки всегда готовы прийти на помощь. Если у вас есть вопросы, свяжитесь с нами удобным вам способом:

- Через систему отправки сообщений на нашем сайте.
- С помощью электронной почты support@nanoav.ru.
- Через Skype “nanoav.support” (только текстовый чат).
- Также вы можете задать вопрос на нашем форуме (для публикации сообщений на форуме необходима регистрация).

Внимание! Набор доступных для связи со службой технической поддержки каналов зависит от типа вашей лицензии!

В ряде случаев при возникновении неполадок в работе антивируса службе технической поддержки требуется расширенная информация для анализа и решения проблемы.

Для сбора и отправки логов, которые содержат необходимую информацию, выберите команду **Сообщить о проблеме в службу поддержки** (меню Пуск>Все программы>NANO Антивирус/NANO Антивирус Pro). По этой команде будет запущена утилита NANO Reporter.

Пожалуйста, детально опишите свою проблему в соответствующем поле. Это поможет нам разобраться в причинах появления неполадок.

Обязательно укажите ваши контактные данные. После анализа присланных вами логов мы свяжемся с вами и объясним, как устранить проблему.

Вы можете выбрать, какую именно информацию вы хотите нам отправить. Если вы не желаете отправлять какую-либо информацию, снимите флажки с соответствующих пунктов. Однако помните, что чем полнее полученная нами информация, тем больше вероятность того, что проблема будет оперативно обнаружена и устранена.

Вы можете отправить нам логи напрямую, воспользовавшись опцией «Отправить в службу тех. поддержки», или по электронной почте. Чтобы отправить логи по почте, выберите пункт «Сохранить» и прикрепите получившийся архив к письму. Если у вас настроен почтовый клиент, воспользуйтесь пунктом «Отправить по почте».

Каждому обращению в службу технической поддержки присваивается соответствующий номер, по которому вы можете отслеживать процесс решения проблемы, по поводу которой было создано обращение.

Системные требования

Для использования NANO Антивируса и NANO Антивируса Pro ваш компьютер должен отвечать следующим системным требованиям:

Минимальные требования *

- Операционная система: Windows 7 и выше.
- Процессор: не менее 2 ГГц, поддерживающий инструкции SSE2.
- Оперативная память: не менее 2 Гб.
- Дисковое пространство: не менее 2 Гб свободного места на системном диске.
- Наличие подключения к сети Интернет *.

Рекомендуемые требования

- Операционная система: Windows 10 / Windows Server 2016 и выше.
- Процессор: не менее 3 ГГц, поддерживающий инструкции SSE2.
- Оперативная память: не менее 4 Гб.
- Дисковое пространство: не менее 2 Гб свободного места на системном диске.
- Наличие подключения к сети Интернет.

Поддерживаемые операционные системы

- Windows 10 (32-бит и 64-бит).
- Windows 8 / 8.1 (32-бит и 64-бит).
- Windows 7 (32-бит и 64-бит).
- Windows Server 2008 R2 и выше (32-бит и 64-бит).

*** Примечание:**

Если ваш ПК не отвечает указанным минимальным требованиям, мы не гарантируем корректную работу NANO Антивируса / NANO Антивируса Pro.

Интернет-подключение требуется для:

- активации пробной версии (trial),
- использования динамических лицензий,
- обновления программы. Возможно обновление NANO Антивируса Pro без подключения к сети Интернет при использовании функционала «Офлайн-обновление».

Внимание: Для установки программы требуются права администратора.