PRO32

Total Security

Защита компьютера и ноутбука

Руководство пользователя

Оглавление

1. Введение

Вас приветствует команда PRO32!

Интернет дает вам доступ к большому количеству информации и открывает массу возможностей для бизнес, однако он также подвергает ваш компьютер множеству угроз, связанных с безопасностью и нарушением конфиденциальности, о которых большинство из нас даже не знает. Интернет-угрозы больше не ограничиваются одними лишь вирусами; они также включают в себя шпионское ПО, вредоносный активный код, спам, взломы и т. д. Каждый раз, когда компьютер подключается к Интернету, он становится потенциальной целью для хакеров. Используя легкодоступные инструменты, такие как шпионское ПО, черви и трояны, компьютерные хакеры могут просматривать личные записи, похищать конфиденциальную информацию и получать контроль над вашим компьютером без вашего ведома. Сложные и быстро распространяющиеся интернет-угрозы используют уязвимости программного обеспечения и операционной системы и распространяются с применением различных хакерских методов.

Современные интернет-угрозы требуют упреждающей защиты и мониторинга отклонений в поведении программного обеспечения в системах в сочетании с традиционной защитой от вирусов и программ-шпионов с применением сигнатур.
PRO32 Total Security – это мощное и простое в использовании комплексное решение для обеспечения безопасности, гарантирующее защиту от новых видов угроз. Это решение с централизованным управлением, которое состоит из тесно взаимосвязанных модулей защиты от вирусов, защиты от шпионских программ, защиты от спама, защиты личных данных и брандмауэра.

PRO32 Total Security помогает защитить ваш компьютер от новых возникающих угроз, включая сетевые вирусы, нежелательная электронная почта, неприемлемый контент и шпионское ПО, которые способны поставить под угрозу вашу конфиденциальность. Это позволяет вам полностью контролировать обмен данными как внутри вашего компьютера, так и с внешними получателями.

1.1. Обзор функций

PRO32 Total Security выполняет постоянный мониторинг вашей системы и защищает ее как от известных, так и от неизвестных угроз.

Среди функций PRO32 Total Security:

✓ **Автоматическая защита** – загружается в память при запуске Windows и обеспечивает непрерывную защиту во время работы; также отслеживает вашу систему на наличие необычных симптомов, которые могут указывать на присутствие угрозы

✓ **Полная защита при доступе** – обеспечивает максимальную защиту, сканируя каждый открываемый, выполняемый или сохраняемый файл; также предотвращает открытие или выполнение зараженных файлов

✓ **Интеграция с почтовыми клиентами** – добавление кнопок на панель инструментов поддерживаемых почтовых клиентов **Полная онлайн-защита электронной почты** – проверяет все входящие и исходящие сообщения электронной почты, обеспечивая полную защиту от соответствующих угроз.

✓ **Защита программ для мгновенного обмена сообщениями** – сканирует и обнаруживает вирусы во вложениях электронной почты и в программах для мгновенного обмена сообщениями

✓ **Защита от троянов** – обнаруживает активность троянов и восстанавливает системные файлы, модифицированные троянами

✓ **Эвристический анализ –** обнаруживает и блокирует многие эксплойты браузера нулевого дня, включая автоматическую загрузку вредоносного ПО.

✓ **Блокировка угроз нулевого –** механизм упреждающей защиты позволяет продукту обнаруживать и блокировать атаки нулевого дня с помощью эксплойтов на основе PDF.

✓ **Защита от хакеров** – скрывает компьютер от хакеров; автоматически определяет приложения, которым разрешено подключаться к Интернету

✓ **Защита параметров безопасности системы** – предотвращает несанкционированные изменения параметров безопасности системы

✓ **Блокировка устройства –** позволяет устанавливать права чтения/записи/исполнения для внешних устройств, таких как USB-накопители, CD/DVD-диски, дискеты

✓ **AutoScanUSB** – сканирует USB-диски сразу после их подключения

✓ **Защита от автоматического выполнения–** отключает функцию автоматического выполнения для всех съемных накопителей на компьютере.

✓ **Вакцинация USB-устройств–** эта функция обеспечивает, что после *вакцинации* USB-накопителя он не сможет автоматически заражать любые ПК, к которым его подключают, с использованием механизма автоматического выполнения.

✓ **Защита USB-устройств паролем –** позволяет настроить парольную защиту в системе, в которой установлен продукт, перед доступом к определенному типу устройства.

✓ **Интеллектуальный брандмауэр** – выполняет мониторинг и защищает вашу систему от интернет-атак и подозрительного поведения.

✓ **Идентификация сети** – обнаруживает тип сети, к которой вы подключаетесь, и назначает соответствующий профиль.

✓ **Режим полной скрытности при прямом подключении** к **Интернету –** брандмауэр включает режим скрытности для всех прямых подключений к Интернету

✓ **Обнаружение вторжений** – контролирует приложения, которым разрешен доступ в Интернет, а также автоматически обнаруживает и блокирует любые интернет-атаки.

✓ **Защита от шпионского и рекламного ПО** – обнаруживает и удаляет шпионское и рекламное ПО, кейлоггеры и прочие интернет-угрозы, которые могут скрыто устанавливаться при загрузке программ из Интернета.

✓ **Автоматическая** идентификация **конфиденциальной информации – выявляет** конфиденциальную информацию по мере ее ввода и предлагает сохранить ее в список контроля конфиденциальности.

✓ **Контроль конфиденциальности**– вы можете настроить параметры конфиденциальности, чтобы быть уверенными, что ваша личная информация останется конфиденциальной и не будет отправлена с компьютера без вашего ведома.

✓ **Списки разрешений и блокировок** – система позволяет настраивать списки индивидуальных адресов электронной почты или целых доменов, с которых вы хотите получать или блокировать сообщения

✓ **Сканер уязвимостей** – выявляет и информирует пользователей о уязвимых прикладных модулях, которые могут быть использованы злоумышленниками для компрометации системы.

✓ **Исправления уязвимостей –** идентифицирует уязвимости и предлагает шаги по исправлению

системы для защиты от таких уязвимостей.

✓ **База данных доверенных интернет- приложений –** PRO32 Total Security в фоновом режиме идентифицирует доверенные приложения, когда они пытаются подключиться к Интернету, и создает соответствующее правило для разрешения доступа

✓ **Диспетчер обновлений рабочего стола –** эта функция позволяет загружать обновления в одну систему и отправлять загруженные обновления в другие системы с помощью диспетчера обновлений рабочего стола.

✓ **Правила** для **спама** – позволяет определять пользовательские правила для идентификации нежелательной почты.

✓ **Интеллектуальный анализ** – использует самообучающиеся байесовские алгоритмы для распознавания нежелательной почты.

✓ **Онлайн- анализатор спама** – сравнивает полученные электронные письма с актуальной централизованной информацией о спаме, хранящейся в онлайн-лаборатории, для выявления нежелательных почтовых сообщений, рассылаемых в различных частях мира.

✓ **Автоматическая обработка угроз** – автоматически восстанавливает или удаляет зараженные файлы и прочие угрозы, такие как трояны, черви и шпионское ПО.

✓ **Автоматическое обновление** – автоматически обновляет и устанавливает копии файлов определений вирусов и нежелательной почты.

✓ **Сканер руткитов** – глубокое сканирование на наличие руткитов можно использовать для общего сканирования системы.

✓ **Отслеживающие файлы cookie** – фрагменты информации, сохраняемые на компьютере браузером, которые позволяют веб-сайту однозначно идентифицировать пользователя.

✓ **Блокировщик фишинговых сайтов** – защищает от веб-сайтов, созданных для того, чтобы вынудить вас обманным путем поделиться личной или финансовой информацией.
✓ **Блокировщик вредоносных сайтов –** защищает от веб-сайтов, потенциально содержащих код, который может быть загружен на компьютер без вашего согласия.

✓ **Игровой режим** – при включении игрового режима продукт не отображает предупреждений или всплывающих сообщений, чтобы не отвлекать вас от игры.

✓ **Нежелательные записи реестра** – сканирует реестр Windows на наличие записей реестра, оставленных вредоносными или нежелательными программами.

✓ **Сканирование нежелательных файлов–** сканирует остаточные файлы, оставленные вредоносными или нежелательными программами.

✓ **Защита паролем** – теперь у пользователей есть возможность установить пароль для изменения настроек, отключения функций и удаления продукта.

✓ **Инструменты.** – продукт поставляется с множеством полезных инструментов, включая средство очистки временных файлов Windows, средство очистки журнала Internet Explorer, средство очистки журнала действий, виртуальная клавиатура и т. д.

✓ **Защита в Интернете –**обеспечивает защиту от веб-сайтов, которые могут нанести вред вашему компьютеру и похитить вашу конфиденциальную информацию

✓ **Data Locker** – обеспечивает защиту от программ-вымогателей, шифруя важные файлы и документы.

✓ **Wi-Fi Security Advisor** – предупреждает о подключении компьютера/ноутбука к потенциально небезопасной беспроводной сети или точке доступа без надежных учетных данных безопасности.

✓ **Защита веб-камеры** – позволяет пользователю блокировать любое несанкционированное использование веб-камеры хакерами или ненадежными приложениями для предотвращения шпионажа.

1.2. Системные требования

Проверьте, соответствует ли компьютер минимальным системным требованиям, указанным ниже.

Поддерживаемые операционные системы:

- Windows XP SP3 (32-разрядная)
- Windows Vista SP2
- Windows 11/10/8.1/8/7

Требуется для всех вариантов установки:

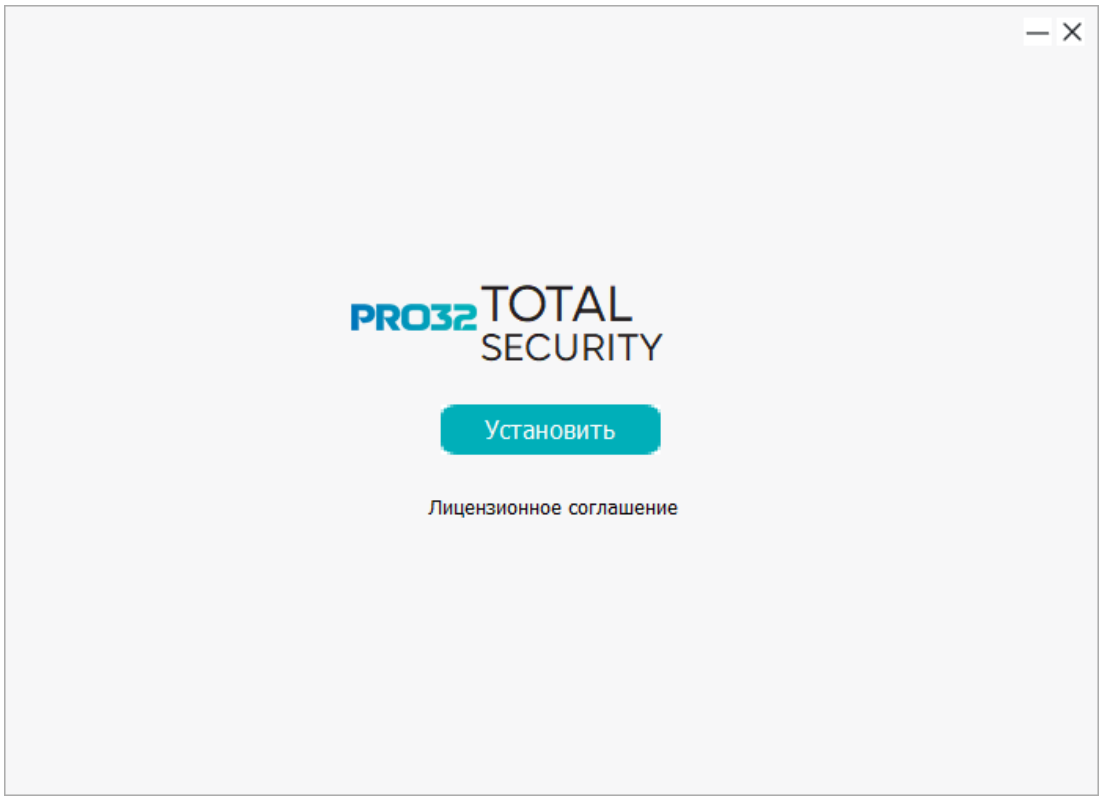
- Дисковод CD/DVD для установки с компакт-диска
- Минимум 1 ГБ ОЗУ для 32-битной системы; 2 ГБ ОЗУ для 64-битной системы
- Подключение к Интернету для активации и обновлений

Если на вашем компьютере установлены другие продукты обеспечения безопасности (брандмауэр/антивирусная программа), удалите их с помощью команды **Пуск → Панель управления → Установка и удаление программ.**

Закройте все открытые приложения.

1.3. Установка

При наличии Интернета вы можете загрузить последнюю версию продукта с веб-сайта PRO32, в противном случае установите его с компакт-диска или другого носителя, появится следующее стартовое окно:



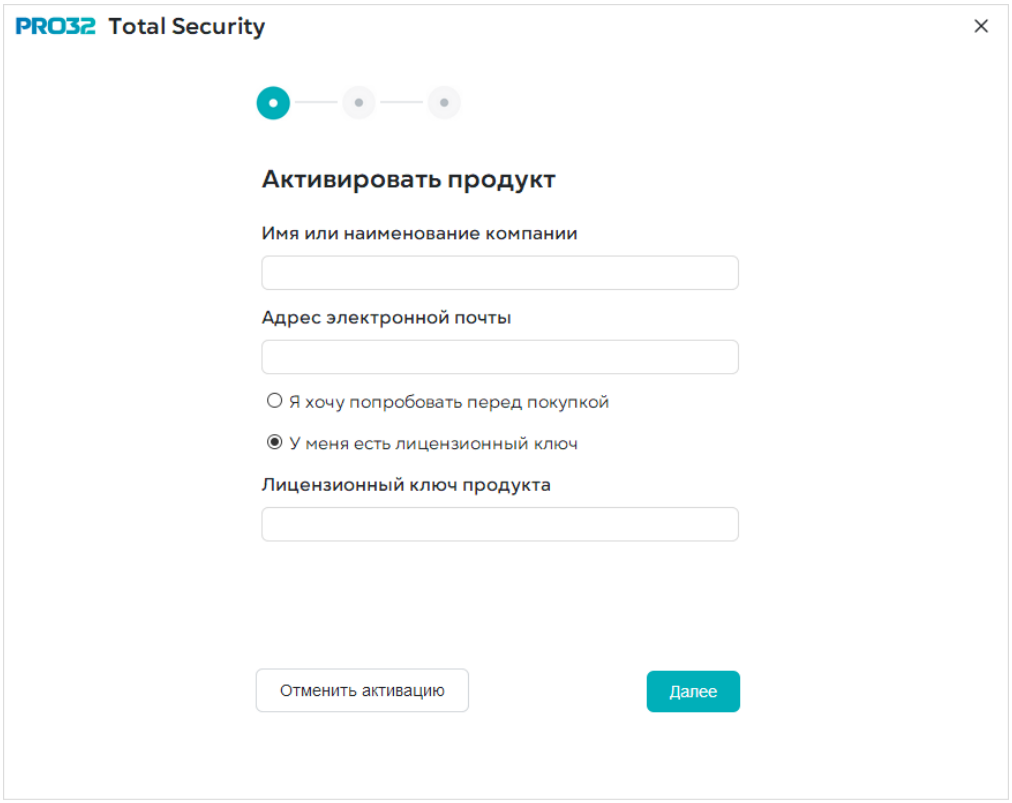
Нажмите «**УСТАНОВИТЬ»**, чтобы быстро установить продукт. Для просмотра лицензионного соглашения с конечным пользователем нажмите **«Лицензионное соглашение»**

После прочтения лицензионного соглашения нажмите «**Согласиться и установить»**, и следуйте подсказкам мастера установки, чтобы установить продукт на компьютер.

1.4. Активация

После завершения установки необходимо зарегистрировать и активировать продукт для регулярного получения определений вирусов и обновлений, что обеспечит безопасность системы. Нажмите «**Активировать»**, чтобы запустить процесс активации.

Выберите опцию **«У меня есть лицензионный ключ»** и нажмите «**Далее»** для продолжения установки.

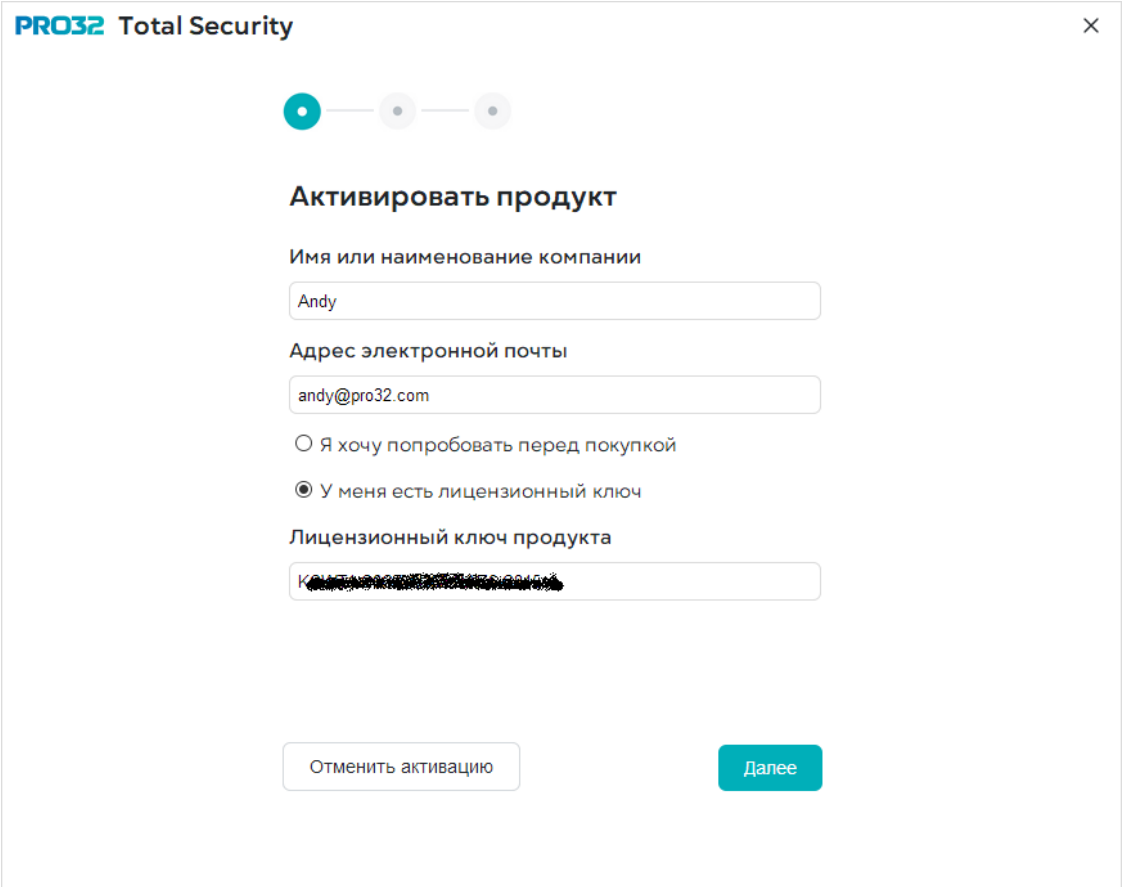


Укажите лицензионный ключ продукта, ваше имя, действующий адрес электронной почты, придумайте пароль укажите номер телефона и нажмите **Далее**.

Совет:

Если вы получили лицензионный ключ в электронном виде и он, например у вас на почте, можно существенно сократить процесс активации. Выделите код в формате XXXXX-XXXX-XXXX-XXXX-XXXX мышью и воспользуйтесь командами Ctrl+C (копировать), затем в поле ввода ключа активации воспользуйтесь командой Ctrl+V (вставить).

Подтвердите указанный адрес электронной почты и номер телефона и нажмите **Далее**. При необходимости изменить какую-либо предоставленную информацию нажмите **Назад**.
При успешной активации на экране появятся ваши регистрационные данные.



Важно! Не забудьте эту информацию. Она потребуется, если вы решите переустановить программу в той же или другой системе.

1.5. Запуск PRO32 Total Security

PRO32 Total Security запускается автоматически вместе с системой. Если по каким-то причинам продукт отключен, запустить PRO32 Total Security можно любым из следующих способов:

1) Нажать Пуск, затем «Программы», затем «PRO32 Total Security», далее «PRO32 Total Security»

2) Дважды нажать левой кнопкой мыши значок на панели задач (в правом нижнем углу)

3) Нажать правой кнопкой мыши значок на панели задач, а затем выбрать вариант «**Открыть PRO32 Total Security**».

Откроется главный экран PRO32 Total Security, на котором будет показан текущий статус вашего продукта.

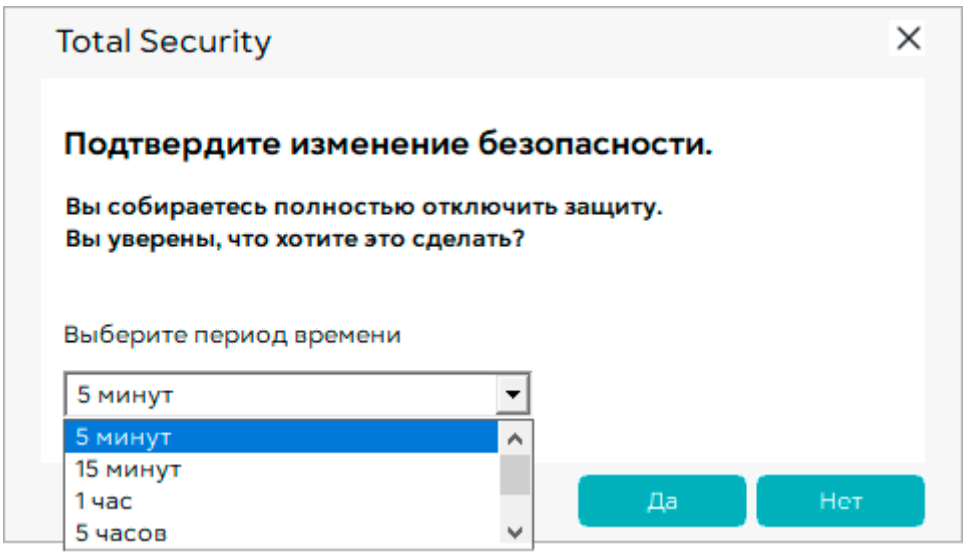
1.6. Отключение PRO32 Total Security

PRO32 Total Security включен по умолчанию. Вы можете отключить продукт.

*Рекомендуется *не отключать* PRO32 Total Security, поскольку это может привести к заражению вашей системы.

Для отключения PRO32 Total Security:

1) Щелкните правой кнопкой мыши значок на панели задач.
2) Нажмите **«Отключить защиту продукта».**
3) Появится подтверждающее сообщение.
4) Выберите время, на которое хотите отключить защиту.



5) Если вы уверены, что хотите отключить PRO32 Total Security, нажмите Да.
6) Если вам нужно краткосрочно отключить PRO32 Total Security, выберите период времени в раскрывающемся списке.
7) Нажмите «Нет», чтобы оставить PRO32 Total Security включенным.

1.7. Игровой режим

Когда включен игровой режим, предупреждения о вирусах и обновления будут отображаться в фоновом режиме, чтобы не отвлекать пользователя от игры. Так же не будет запускаться проверка компьютера.

Для включения игрового режима:

1. Нажмите правой кнопкой мышки значок на панели задач и выберите **«Включить игровой режим».**

2. Пользователь может выбирать продолжительность времени, в течение которого будет действовать игровой режим.

Отключение игрового режима:

Когда игровой режим выключен, предупреждения о вирусах и обновления будут отображаться в штатном режиме.

Для отключения игрового режима:

3. Правой кнопкой нажмите значок на панели задач, нажмите **«Отключить игровой режим».**

1.8. Удаление PRO32 Total Security

Для удаления PRO32 Total Security необходимо войти в систему как администратор. Кроме того, после удаления программного обеспечения вам нужно будет перезагрузить компьютер.

После удаления программы, файлы, помещенные в карантин, смогут свободно распространяться по дискам вашего ПК.

Для удаления PRO32 Total Security:

1. Нажмите **«Пуск»,** затем **«Параметры»**, далее **«Панель управления».**

2. На «Панели управления» дважды нажмите пункт **«Установка и удаление программ».**

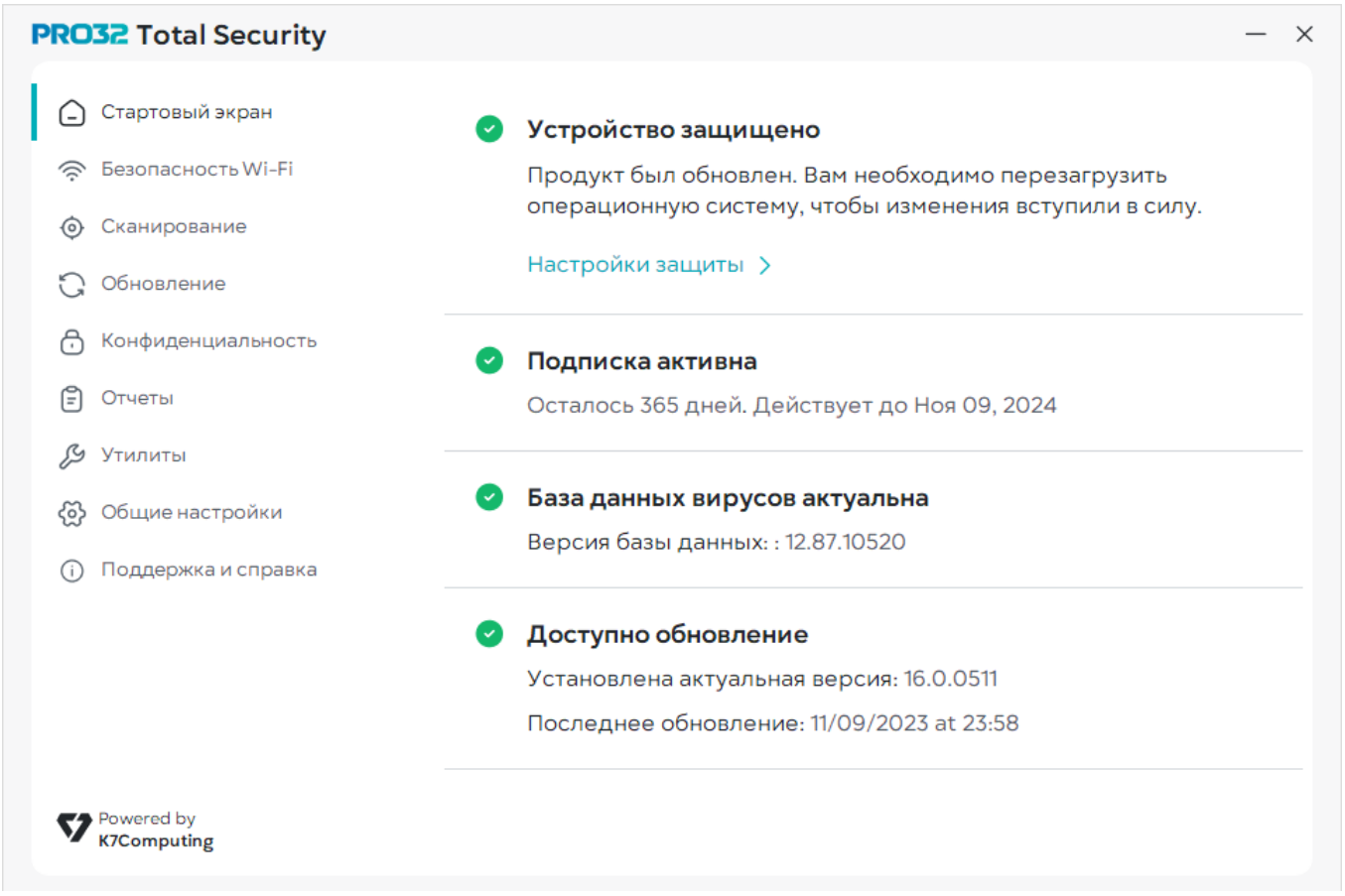
3. Выберите PRO32 Total Security в списке **«Установленные программы»** и нажмите **«Удалить».**

4. Следуйте инструкциям на экране для удаления программного обеспечения.

5. Если по каким-то причинам удаление не происходит, воспользуйтесь специальной утилитой для удаления продукта. Скачать утилиту можно на сайте PRO32.com в разделе **«Скачать для дома и мобильных устройств».**

2. Стартовый экран

Внешний вид главного экрана PRO32 Total Security представлен на следующем рисунке.



Главный (стартовый) экран разбит на две области: слева находится боковая панель со списком модулей, а справа – основное меню управления.

Боковая панель состоит из стартового экрана и модулей Безопасность Wi-Fi, Сканирование, Обновления, Конфиденциальность, Отчёты, Утилиты, Настроек и Резервного копирования.

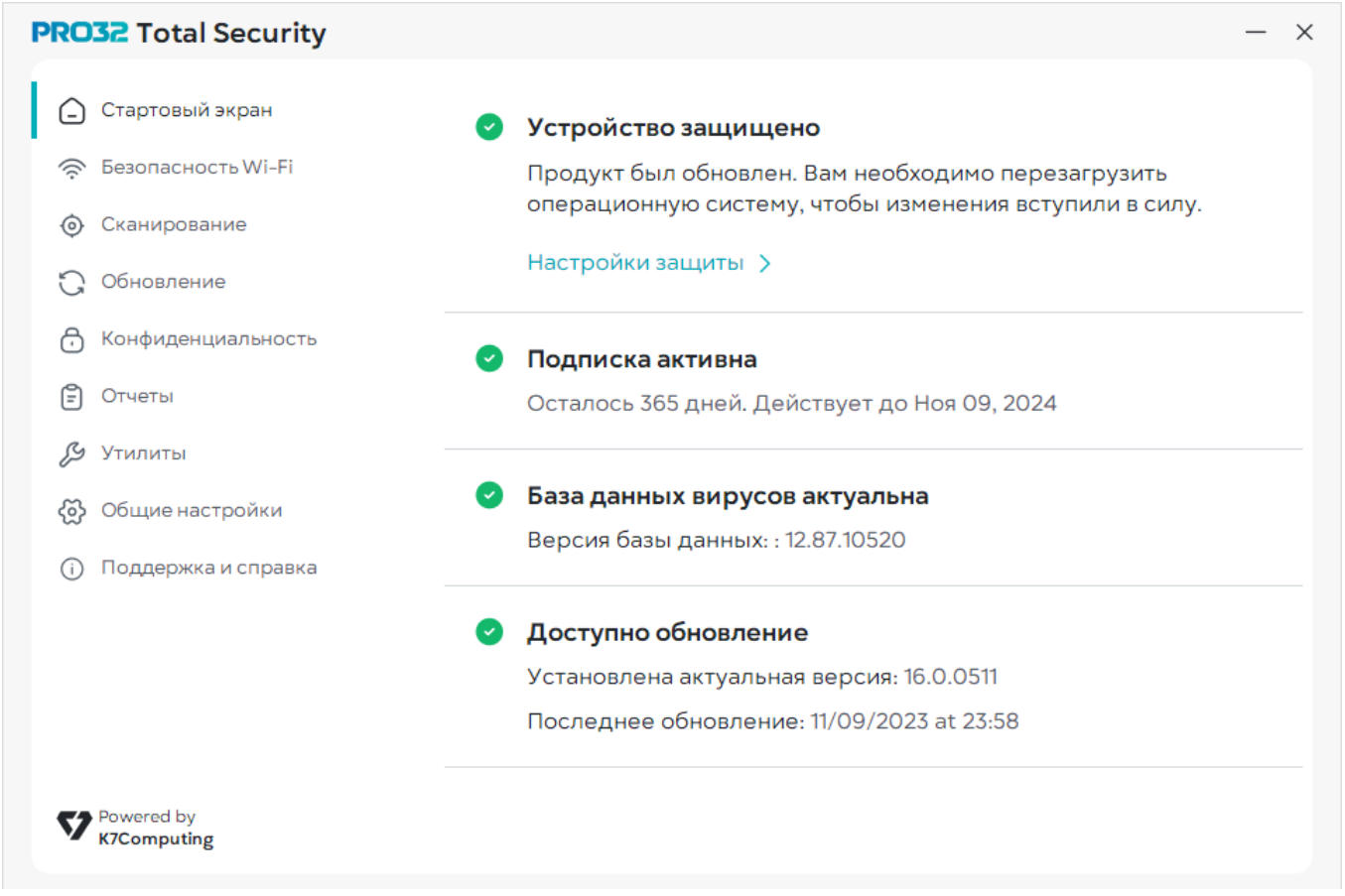
3. Стартовый экран и настойки защиты

Открыть стартовый экран PRO32 Total Security можно любым из следующих способов:

1. Нажать **«Пуск»,** затем **«Программы»,** затем «PRO32 Total Security», далее «PRO32 Total Security»

2. Дважды нажать значок на панели задач

3. Нажать правой кнопкой мыши значок на панели задач, а затем выбрать вариант «**Открыть PRO32 Total Security»**.



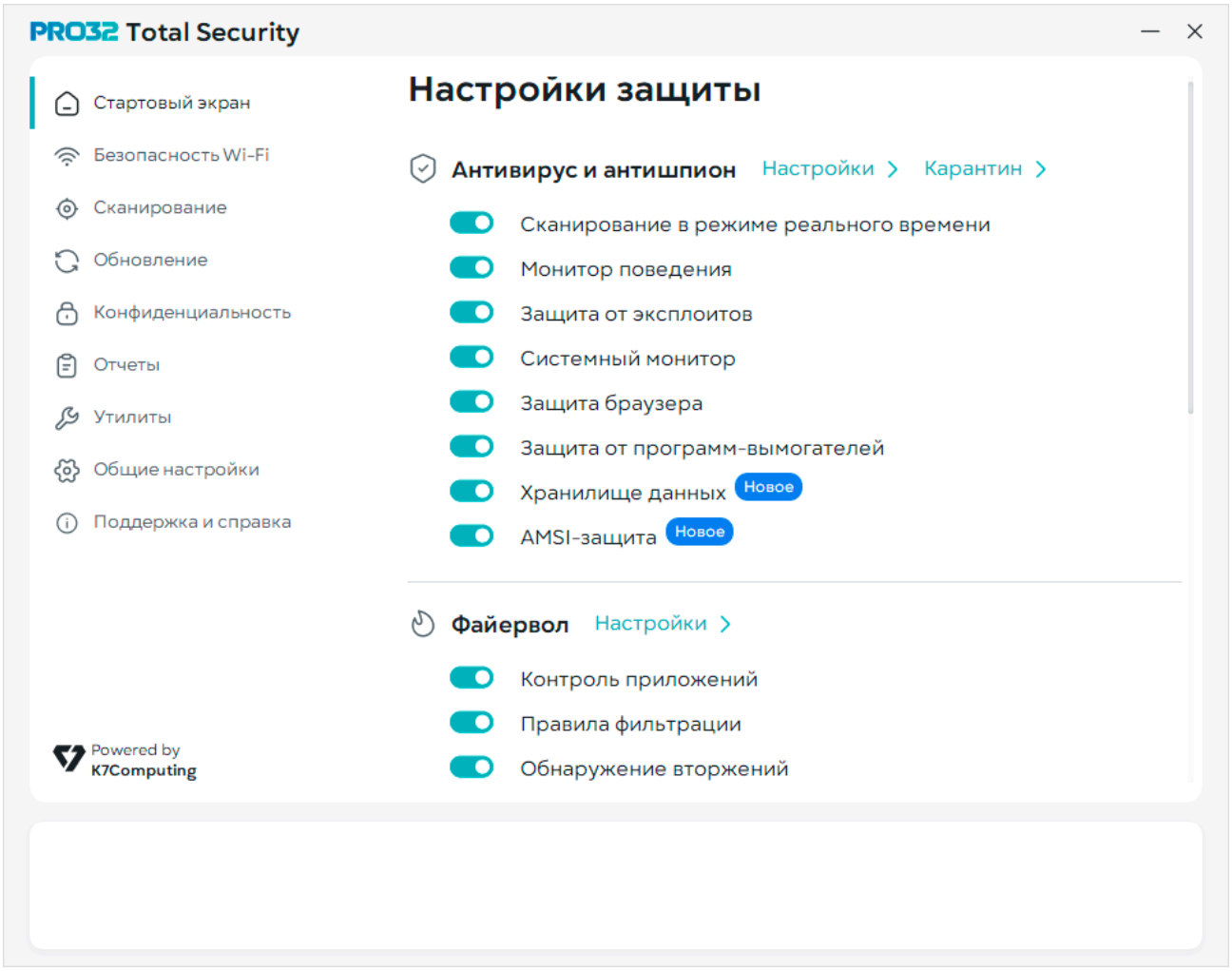
На главном экране отображается сводный статус работы продукта.
Указаны информация о дате и времени последнего обновления, информация о базах вирусных сигнатур и статус лицензии.

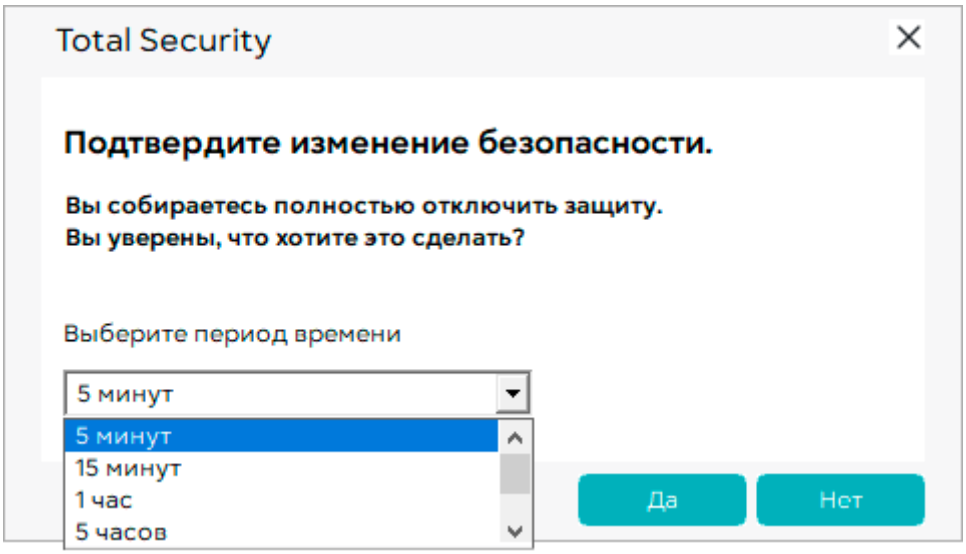
Также на главном экране находится меню **«Настройки защиты».**

4. «Настройки защиты». Управление модулями

В меню «Настройки защиты» показаны включенные и отключенные компоненты продукта. Это основное меню для управления и настоек модулей продукта.

Состояние модулей изображается выключателями . По умолчанию все компоненты и модули продукта включены и имеют преднастроенные правила работы. Для того, чтобы быстро отключить какой-либо модуль, переключите выключатель в состояние «Выкл» . Выберите время, на которое хотите отключить тот или иной модуль и подтвердите выбор кнопкой «Да».





5. Модуль «Антивирус и антишпион»

Модуль «Антивирус и антишпион» обеспечивает надежную и современную защиту от вирусов. Он постоянно сканирует вашу систему в фоновом режиме и предотвращает заражение вирусами из файлов, поступающих через вложения электронной почты, программы мгновенного обмена сообщениями, загрузки из Интернета и через использование уязвимостей. Этот компонент также сканирует систему на наличие определенных невирусных угроз, таких как шпионское ПО, рекламное ПО и прочие средства атаки.

Модуль состоит из компонентов:

1. Сканирование в режиме реального времени

Функция защиты от вирусов (сканирования в режиме реального времени) постоянно контролирует вашу систему на наличие вирусов, сканирует файлы каждый раз, когда вы или ваш компьютер обращаетесь к ним. При обнаружении вируса антивредоносное ПО попытается очистить или удалить инфицированный объект.

2. Сканирование почты

Сканер электронной почты проверяет входящие и исходящие электронные письма, чтобы не допустить попадания зараженных писем в ваш почтовый ящик. Если электронное письмо содержит вирус, сканер электронной почты удаляет зараженные вложения или помещает их в карантин.

3. Монитор поведения

Сканирует подозрительные активности в мессенджерах, а также позволяет сканировать все файлы Word и Excel, открытые в MSOffice.

4. Защита от Эксплойтов

Защита от эксплойтов Эвристический механизм упреждающей защиты, который позволяет продукту обнаруживать и блокировать атаки нулевого дня с помощью эксплойтов на основе PDF.

5. Системный монитор

Системный монитор отслеживает изменения следующих контрольных точек. Вы можете выбрать или отменить выбор этих контрольных точек в зависимости от ваших текущих потребностей.

6. Защита браузера

Обнаруживает и блокирует многие эксплойты браузера нулевого дня, включая автоматическую загрузку вредоносного ПО.

7. Защита от программ-вымогателей (Сейф)

Система защиты от программ-вымогателей на основе мониторинга поведения блокирует распространение и шифрование файлов программой-вымогателем.

8. Хранилище данных

Позволяет контролировать доступ к USB-накопителям, CD-, DVD-дискам и дисководам гибких дисков. Вы можете управлять возможностью копирования файлов на диск или с диска, а также возможностью их выполнения. Кроме того, доступ к этим дискам можно защитить паролем.

9. AMSI-защита

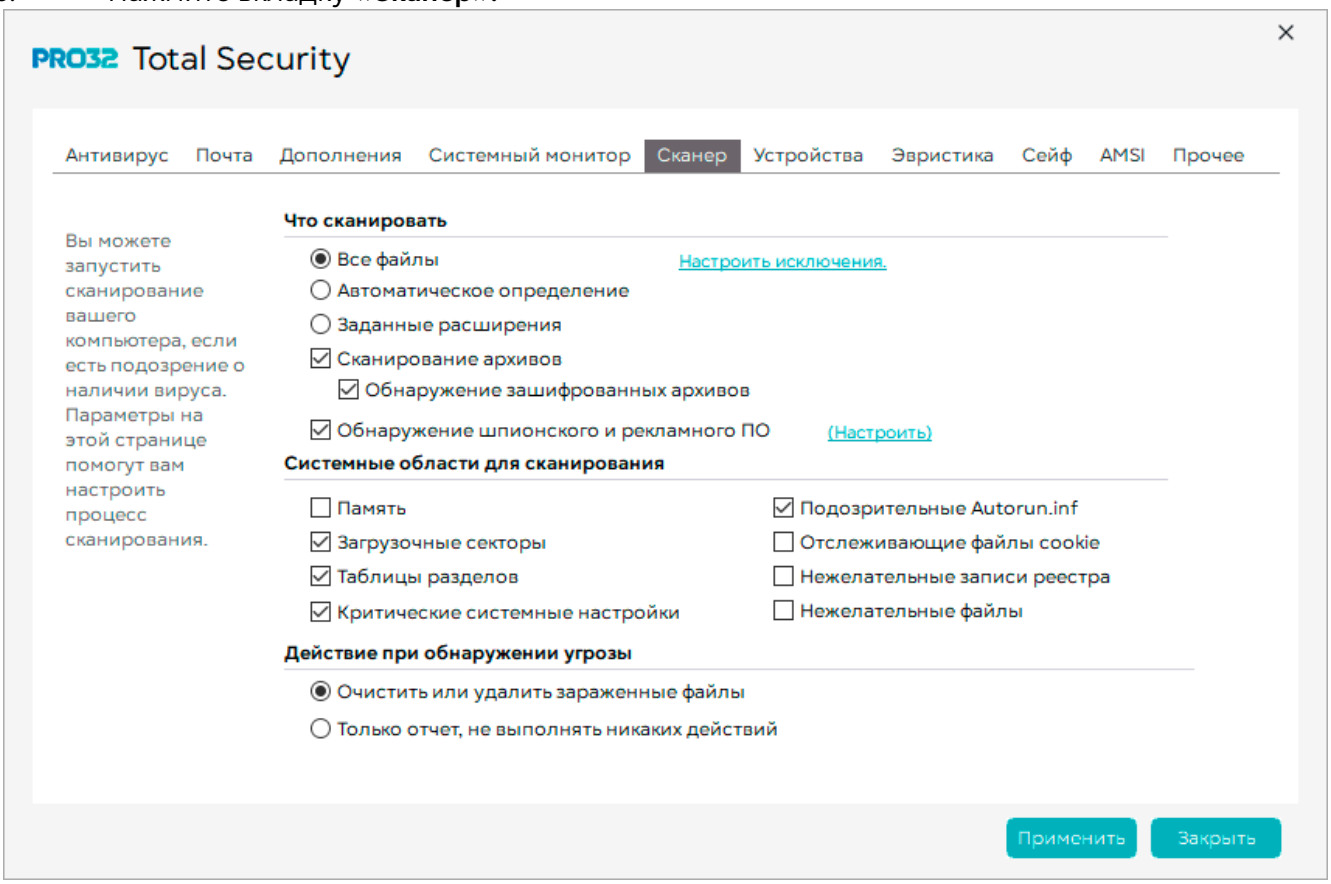
Позволяет защитить ваш компьютер от угроз, использующих легитимное программное обеспечение. Нажмите кнопку **«Настройки»,** чтобы изменить работу каждого из вышеперечисленных модулей.

5.1. Настройка параметров сканирования

По умолчанию антивирусное сканирование проводится автоматически. Вы можете настроить сканирование вручную или по расписанию, необходимо указать типы файлов для сканирования, сканируемые системные области и действие, которое необходимо предпринять в случае обнаружения вируса или угрозы.

Для настройки параметров сканирования:

1. Откройте стартовый экран продукта, затем **«Настройки защиты»** > , далее **«Настройки»** > модуля **«Антивирус и антишпион»** .
2. Откроется диалоговое окно настроек антивируса.
3. Нажмите вкладку **«Сканер».**



На панели «Что сканировать выберите» типы файлов для сканирования.

Все файлы

Сканирует все файлы в системе независимо от их расширения или типа

Автоматическое определение

Сканирует все исполняемые (программные) файлы, файлы документов Microsoft и файлы сценариев независимо от того, указаны ли их расширения. Нажмите «Настроить» рядом с этим параметром, чтобы выбрать типы файлов для сканирования.

Заданные расширения

Сканирует файлы с указанными расширениями. Чтобы указать расширение, нажмите пункт Настроить, отображаемый рядом с расширением. Можно просматривать, добавлять или удалять сканируемые расширения.

Выполнять сканирование в архивах

Сканирует файлы в архивах на наличие вирусов и угроз

Обнаружение шпионского и рекламного ПО

Сканирует выбранные файлы на наличие дополнительных угроз, включая шпионское ПО, рекламное ПО, дозвонщики и т. д. Установите флажок, а затем щелкните пункт настроить, который

появляется рядом с ним, чтобы настроить тип сканируемых угроз и действие, которое необходимо предпринять при обнаружении угрозы.

Память

Проверяет память вашего компьютера на наличие вирусов

Загрузочные секторы

Проверяет наличие загружаемых вирусов в загрузочных секторах сканируемого жесткого диска или дискеты.

Таблицы разделов

Проверяет наличие вирусов в таблице разделов жесткого диска

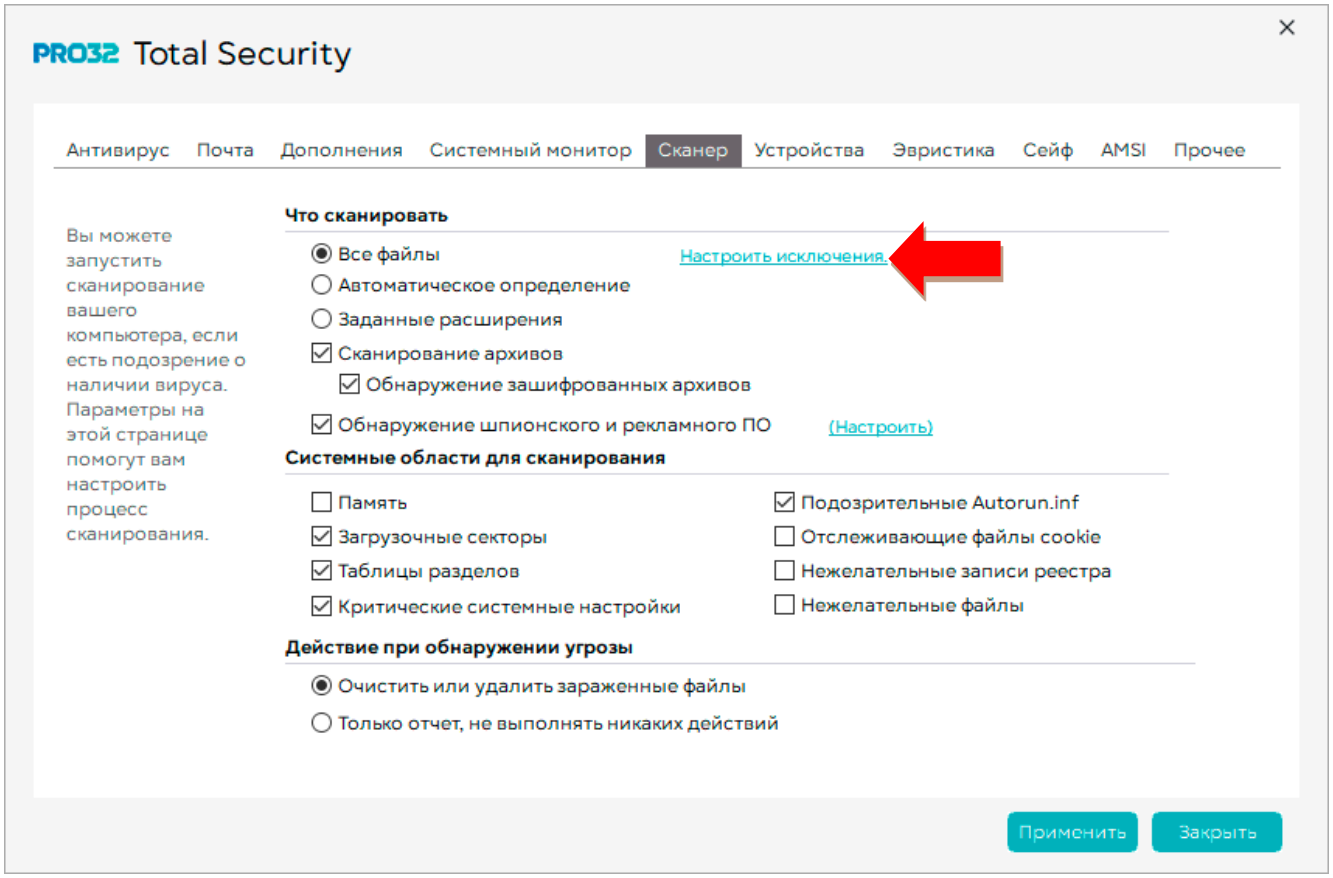
5.1.1. Управление исключениями

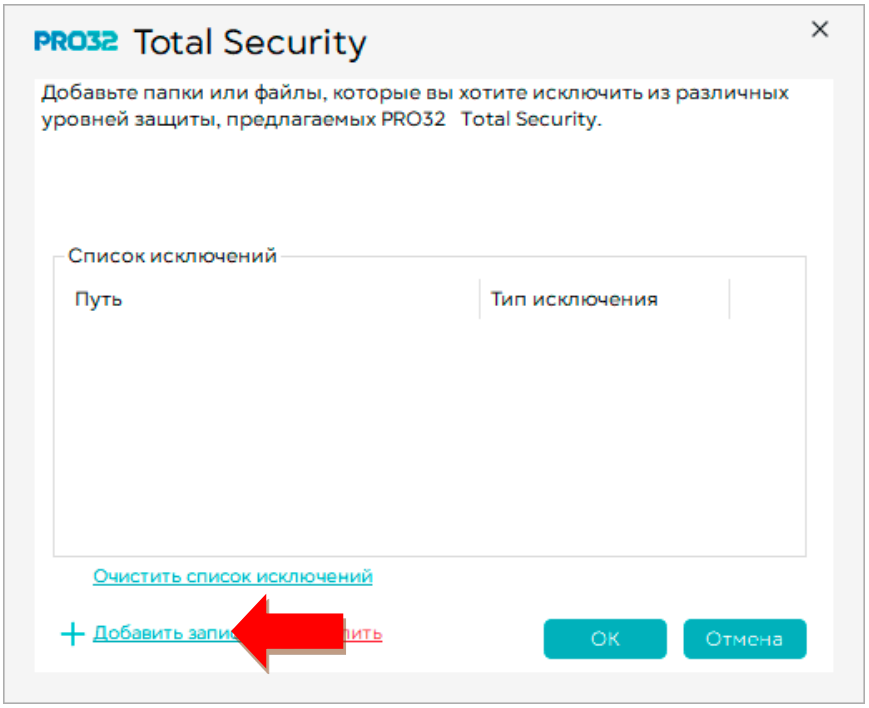
Вы можете исключить определенные файлы и области, например, папки или программы, из сканирования. Функция полезна, если вы используете специфическое ПО, на которое происходит ложное срабатывание антивируса.

1. Откройте стартовый экран продукта , затем **«Настройки защиты»** , далее **«Настройки»** модуля **«Антивирус и антишпион»** .

2. Откроется диалоговое окно настроек антивируса.

3. Нажмите вкладку **«Сканер»,** затем **«Настроить исключения».**





1. Чтобы добавить папки или файлы, исключаемые из защиты, нажмите «**Добавить запись**» +.

2. В появившемся диалоговом окне «Добавить новую запись для исключения» введите путь к папке или файлу. Если вы не уверены в точном пути к объекту, нажмите «**Добавить папку**» или «**Добавить файл**», чтобы выбрать папки или файлы соответственно.

3. Чтобы удалить все исключенные записи, добавленные из окна результатов сканирования, выберите «**Очистить список исключений».**

4. Выберите следующие параметры:

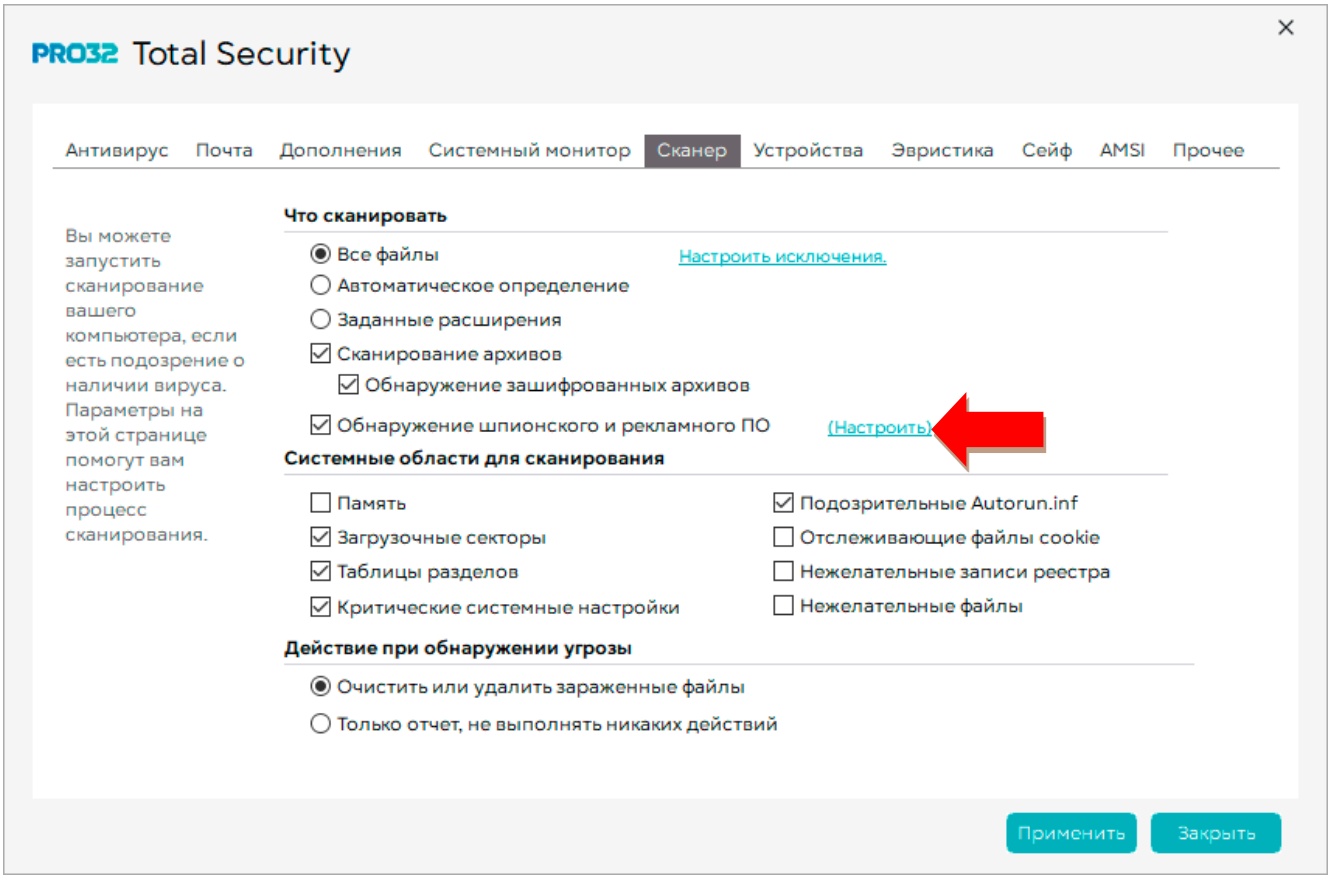
- **Исключить из сканирования в реальном времени** – чтобы исключить выбранный файл или папку из **сканирования** в реальном времени.
- **Исключить из оффлайн сканера** – чтобы исключить выбранный файл или папку из **автономного** сканирования.
- **Включить подпапки** – чтобы исключить из сканирования вложенные папки в выбранной папке. Этот параметр недоступен, если файл выбран в качестве исключения.

5. Нажмите «**ОК»**, чтобы сохранить новую запись и вернуться в диалоговое окно «Список исключений».
6. Чтобы удалить файл или папку из списка исключений, выберите запись в списке и нажмите **Удалить**.
7. Нажмите **«ОК»** для сохранения настроенных исключений.

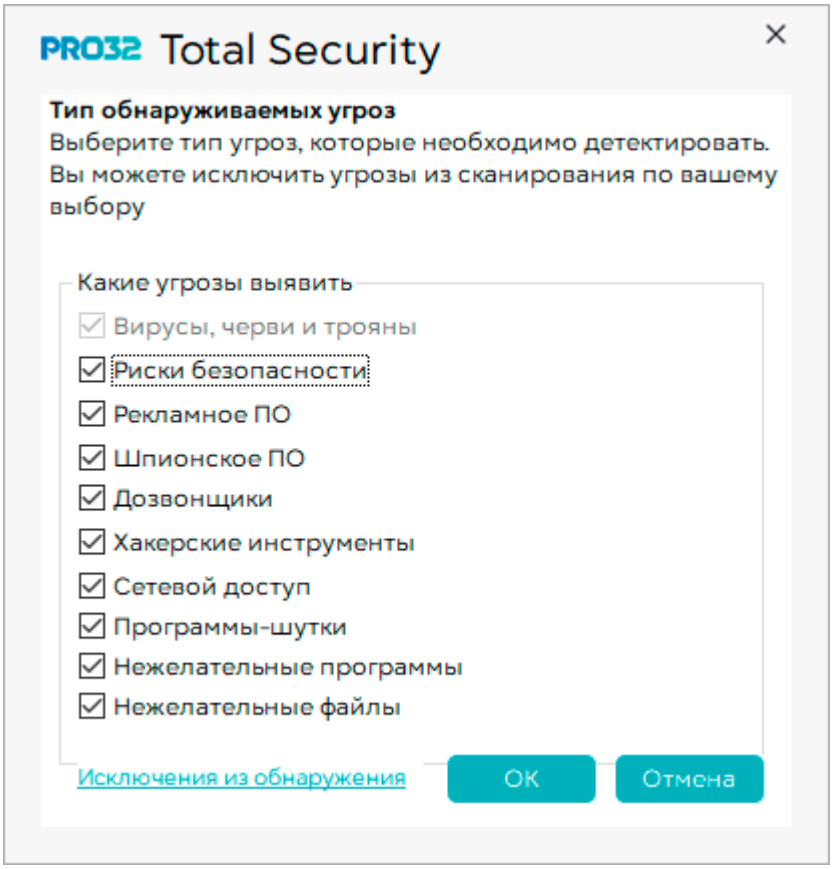
5.2. Блокировка по категориям

Вы можете исключить определенные файлы и области, например, папки или программы, из сканирования

1. Откройте стартовый экран продукта, затем **«Настройки защиты»** > , далее **«Настройки»** > модуля **«Антивирус и антишпион»** .
2. Откроется диалоговое окно настроек антивируса.



3. Нажмите вкладку **«Сканер»,** затем **«Настроить»** (напротив опции **«Обнаружение шпионского и рекламного ПО»**).



Выберите тип угроз, которые необходимо детектировать. Вы можете исключить категории угроз из сканирования по вашему выбору:

Вирусы, черви и трояны

Вирусы, трояны и интернет-черви. Эти угрозы сканируются по умолчанию.

Риски для безопасности

Известные программы, которые могут представлять или не представлять опасность для вашего компьютера, при этом обладают свойствами червя

Шпионское ПО

Автономные программы, которые отслеживают активность вашей системы в фоновом режиме, а также способны обнаруживать и отправлять конфиденциальную информацию, например, пароли, с вашего компьютера.

Рекламное ПО

Автономные программы, предназначенные для отображения рекламных баннеров во время работы программы. Эти программы обычно содержат код, отслеживающий личную информацию пользователя и передающий ее третьим лицам.

Дозвонщики

Программы, которые без вашего ведома звонят на другие уязвимые сайты или FTP-узлы, в основном для взимания платы.

Программы-шутки

Программы, которые изменяют нормальное функционирование вашей системы, например, включают залипание клавиш или меняют назначение функциональных клавиш.

Доступ к сети

Программы, которые позволяют другим получать доступ к вашему компьютеру через Интернет с целью сбора информации или проведения атак на ваш компьютер.

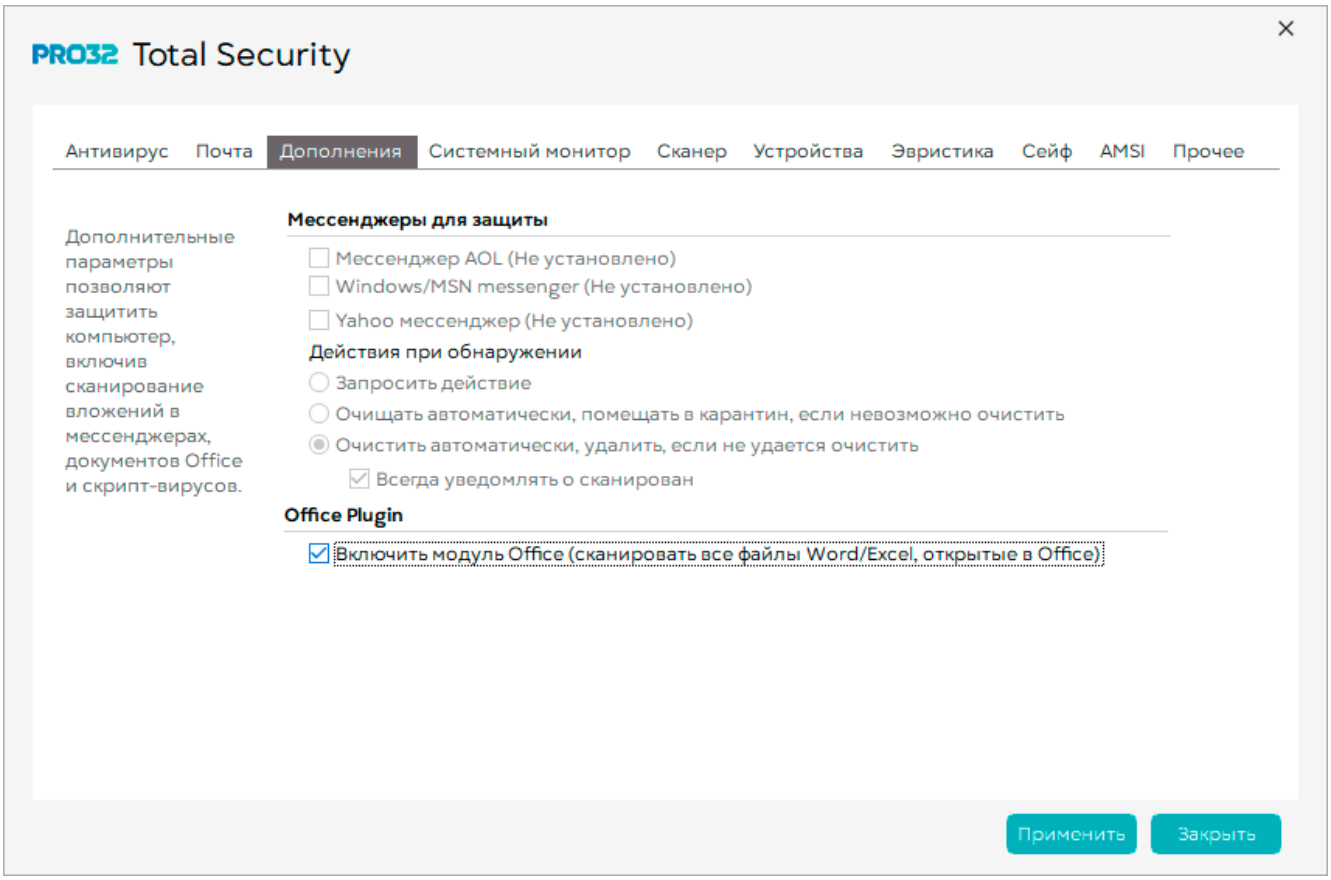
Хакерские инструменты

Программы или инструменты, используемые хакерами для получения несанкционированного доступа к вашим компьютерам. Это могут быть простые регистраторы клавиатуры, которые фиксируют нажатия клавиш и отправляют информацию хакеру.

5.3. Настройка дополнений

Дополнительные параметры сканирования позволяют защитить компьютер за счет сканирования вложений в мессенджерах и документов Office.

1. Откройте стартовый экран продукта , затем **«Настройки защиты»** , далее **«Настройки»** модуля **«Антивирус и антишпион»** .
2. Откроется диалоговое окно настроек антивируса.
3. Нажмите вкладку **«Дополнения».**



Можно настроить сканирование

• Программ обмена мгновенными сообщениями.

• Файлов Office (Word/Excel).

4. Нажмите «Применить» для сохранения настроек.

5. Нажмите «Закрыть» для закрытия диалогового окна защиты от вредоносного ПО

5.4. Настройка системного монитора

Системный монитор постоянно отслеживает критически важные области вашего компьютера и предупреждает о последствиях любых изменений, внесенных в вашу систему. Это помогает в раннем обнаружении вирусов и защищает ваш компьютер от скрытых угроз до их запуска.

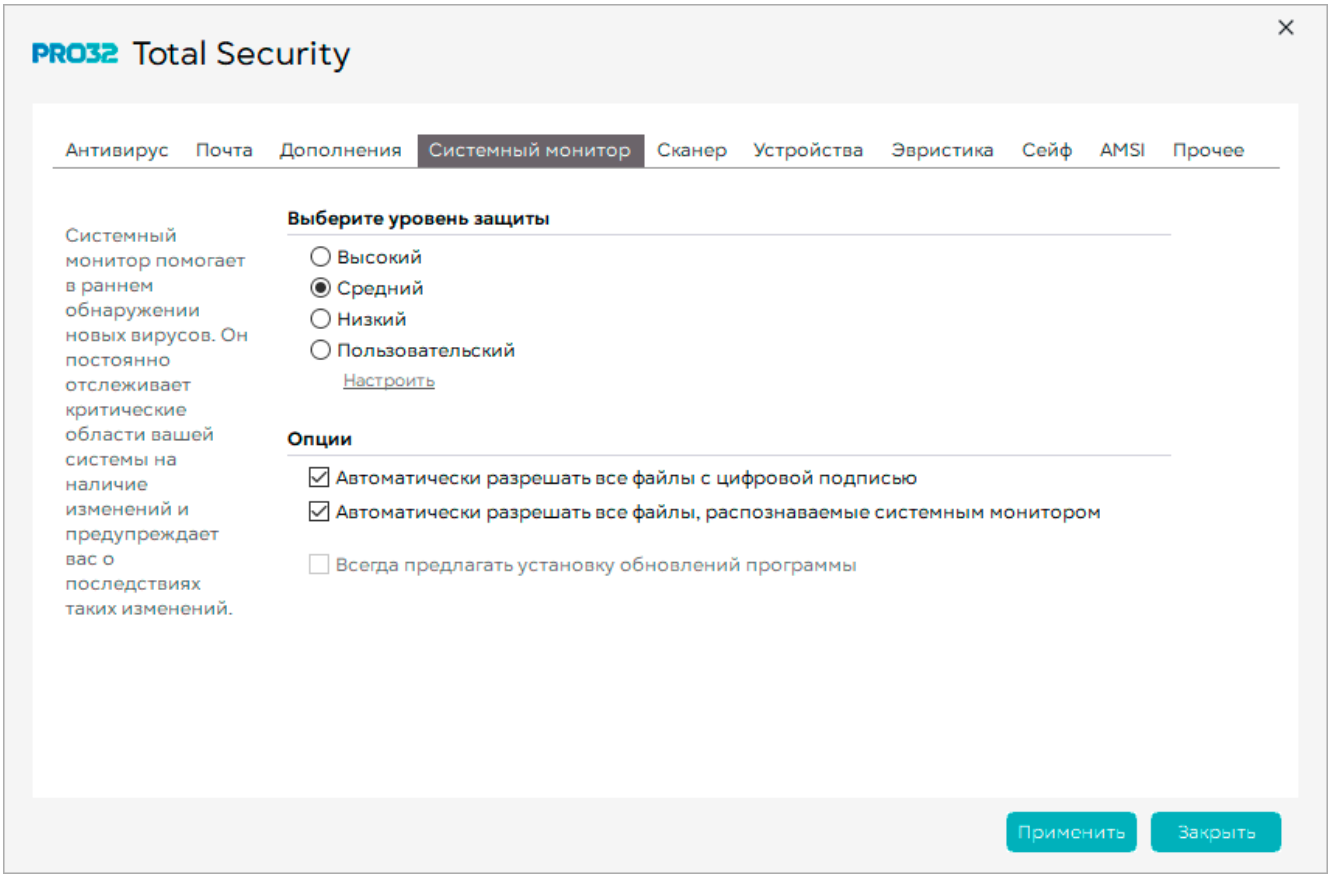
Для настройки системного монитора:

1.Откройте стартовый экран продукта , затем **«Настройки защиты»** , далее **«Настройки»** модуля **«Антивирус и антишпион»** .

2. Откроется диалоговое окно настроек антивируса.

3. Нажмите вкладку «Системный монитор».

4. Выберите Уровень защиты, который системный монитор должен использовать при проверке на наличие шпионских программ.



Уровень защиты:

Высокий

Отслеживает все контрольные точки на наличие шпионского ПО

Средний

Отслеживает большинство контрольных точек, кроме точек, не имеющих критического значения

Низкий

Отслеживает только контрольные точки, имеющие наиболее критическое значение

По выбору пользователя

Позволяет выбрать контрольные точки, которые будет проверять системный монитор в соответствии с имеющимися требованиями.

5. Чтобы установить дополнительные Параметры, установите\снимите необходимые флажки:

Автоматически разрешить все файлы с цифровой подписью

Разрешает все файлы, имеющие цифровую подпись

Автоматически разрешать все файлы, распознаваемые системным монитором

Разрешает все файлы, распознанные системным монитором

Всегда показывать уведомление в случае обнаружения изменений при установке нового программного обеспечения

Отображает уведомление если обнаруженные изменения указывают на установку нового программного обеспечения. Это вариант выбирается автоматически, когда установлен уровень защиты высокий.

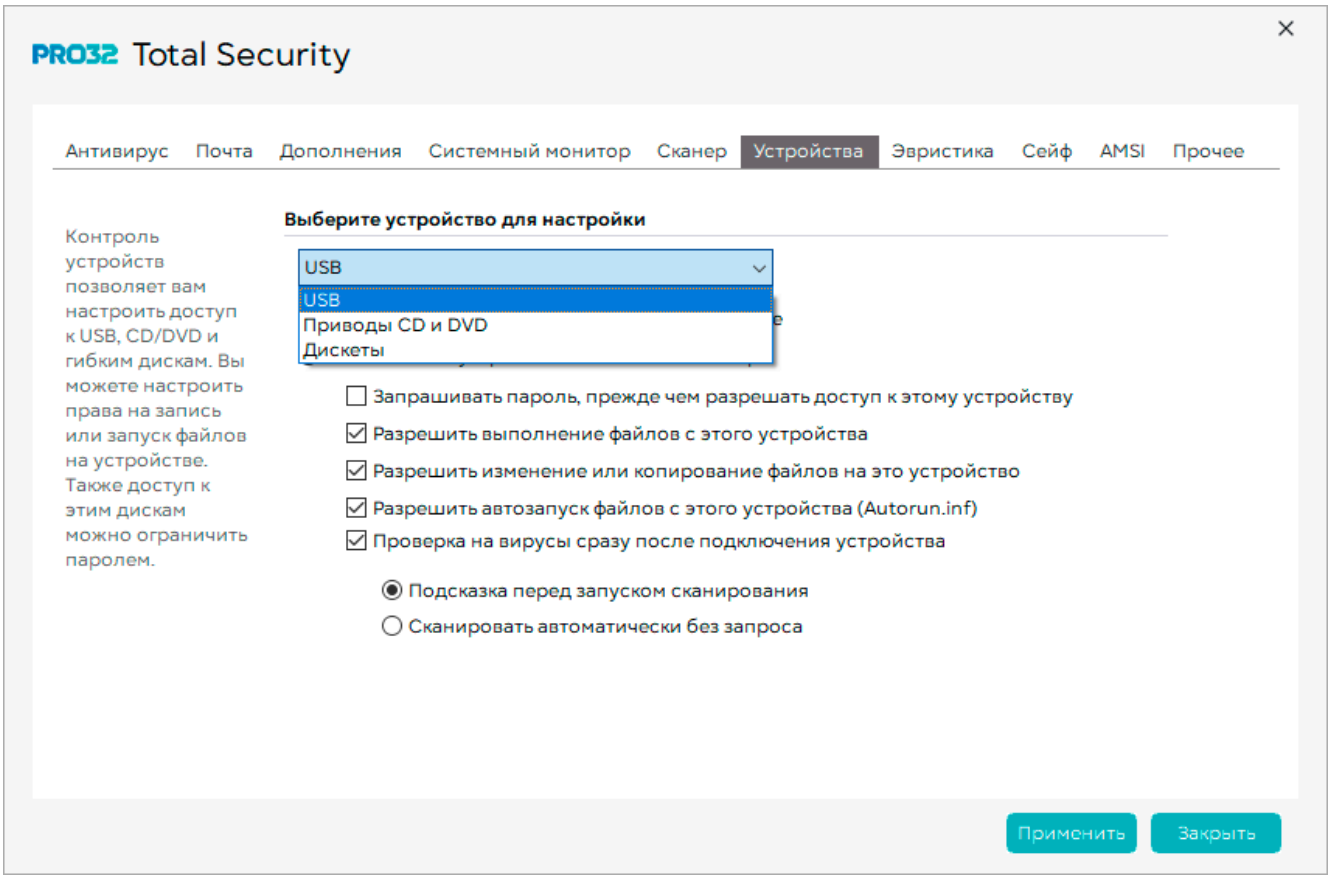
6. Нажмите «Применить» для сохранения настроек.

5.5. Настройка доступа к устройствам

С ростом числа вредоносных программ, способных заражать вашу систему через такие устройства, как USB, важно обеспечить защиту доступа к этим устройствам. Функция доступа к устройствам позволяет контролировать доступ к USB-накопителям, CD-, DVD-дискам и дисководам гибких дисков. Вы можете управлять возможностью копирования файлов на диск или с диска, а также возможностью их выполнения. Кроме того, доступ к этим дискам можно защитить паролем.

Для включения управления внешним устройством:

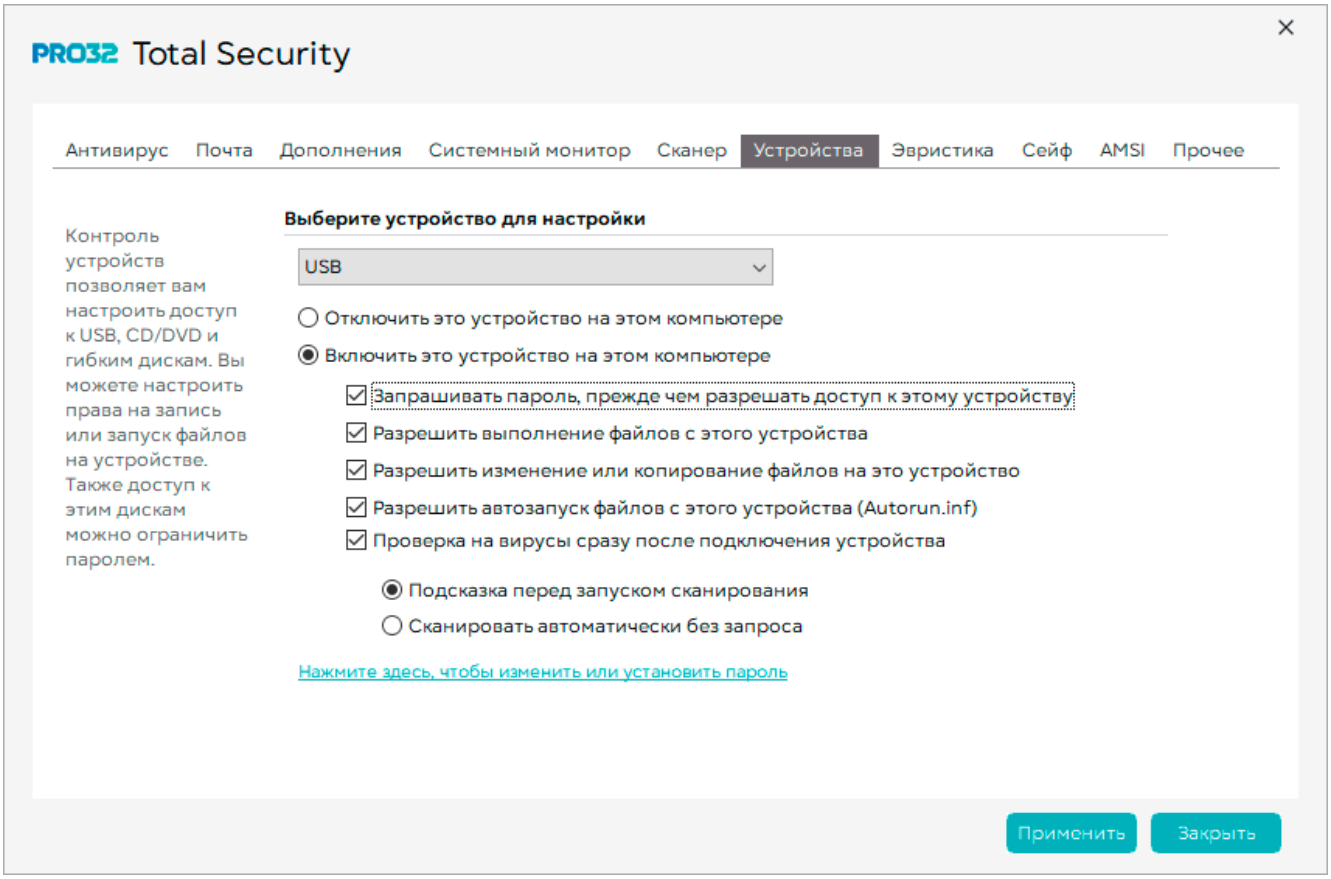
1. Откройте стартовый экран продукта, затем **«Настройки защиты»** > , далее **«Настройки»** > модуля **«Антивирус и антишпион»** .
2. Откроется диалоговое окно настроек антивируса.



3. Нажмите вкладку **«Устройства».**
4. В раскрывающемся списке выберите тип устройства, которое требуется настроить.
5. Включите устройство, выбрав параметр «**Включить это устройство на этом компьютере».**

Настройка пароля для устройства

Вы можете защитить доступ к внешнему устройству с использованием пароля. Это позволит предотвратить несанкционированное использование этих устройств в вашей системе. При подключении выбранного устройства к системе появится запрос на ввод пароля. Если не ввести пароль, то доступ к устройству будет заблокирован.



Чтобы установить пароль для доступа к внешнему устройству:

1.Откройте стартовый экран продукта, затем **«Настройки защиты»** > , далее **«Настройки»** > модуля **«Антивирус и антишпион»** .

2. Откроется диалоговое окно настроек антивируса.

3. Нажмите вкладку «Устройства».

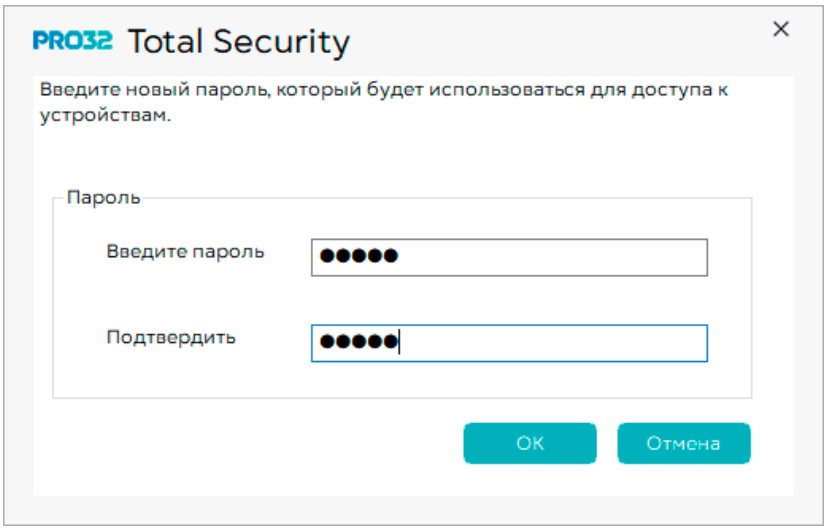
4. В раскрывающемся списке выберите тип устройства, которое требуется настроить.

5. Установите флажок **«Запрашивать пароль, прежде чем разрешать доступ к этому устройству».**

6. Появится ссылка с надписью **«Нажмите здесь, чтобы изменить или задать пароль».**

7. Нажмите кнопку и введите пароль по своему усмотрению.

8. Подтвердите пароль, нажав кнопку **«ОК».**



Запрос пароля устройства

Для этого диска включена защита паролем. Для доступа к устройству введите правильный пароль.

Доступны следующие действия:

1. Введите пароль в поле **с** надписью **«Введите правильный пароль здесь»**.

2. Если вы не хотите, чтобы пароль для того же диска запрашивался **до** перезагрузки **компьютера**, установите флажок **«Больше не запрашивать пароль**, **пока компьютер не будет перезагружен».**

3. Установите флажок **«Сканировать на вирусы сейчас»**, чтобы отсканировать устройство на наличие вирусов.

Нажмите **ОК** для получения доступа к устройству после ввода пароля. Нажмите **Отмена** для выхода

Настройка ограничений доступа для устройств

Вы можете установить ограничение на любые выбранные внешние устройства. Вы можете устанавливать разрешения на такие действия, как чтение, изменение, копирование или выполнение файлов с выбранных внешних устройств.

Для установки ограничений доступа для внешнего устройства:

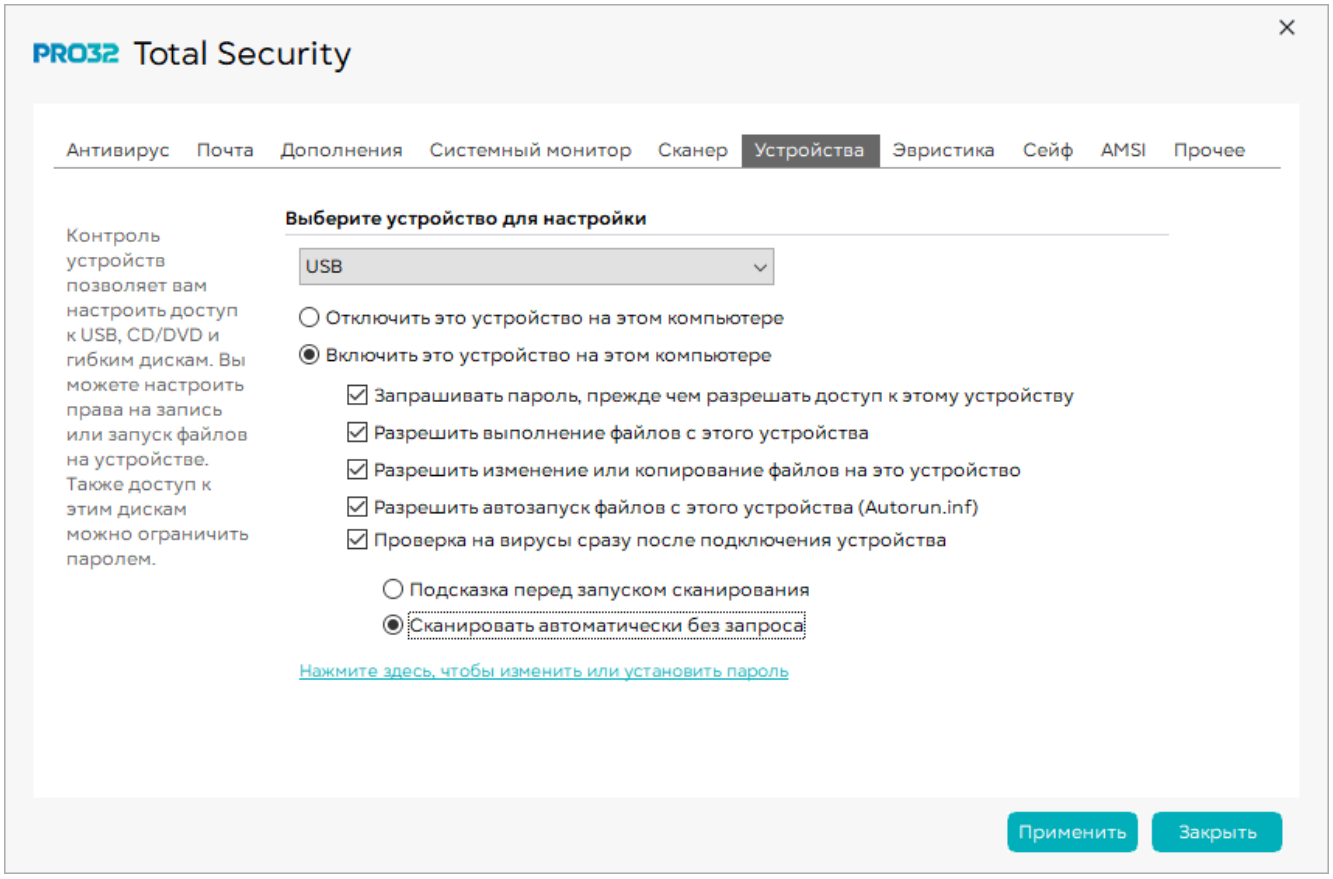
1. Откройте стартовый экран продукта, затем «Настройки защиты», далее «Настройки».
2. Откроется диалоговое окно настроек антивируса.
3. Нажмите вкладку «Устройства».
4. В раскрывающемся списке выберите тип устройства, которое требуется настроить.
5. Если выбрать параметр **«Разрешить выполнение файлов с этого устройства»**, то вы сможете запускать исполняемые файлы **с** выбранного **устройства**.
6. Если выбрать параметр **«Разрешить изменение или копирование файлов на этом устройстве»**, то вы сможете записывать/копировать файлы на выбранное устройство

Настройка автозапуска для устройства

Зараженный файл Autorun.inf – это один из распространенных методов, используемых вредоносными программами для запуска при подключении USB-накопителя к системе. Отключение исполняемых файлов с устройства позволяет предотвратить выполнение автозапуска, а это, в свою очередь, препятствует проникновению вредоносных программ в систему.

Чтобы предотвратить выполнение файлов Autorun.inf:

1. Откройте стартовый экран продукта, затем **«Настройки защиты»** > , далее **«Настройки»** > модуля **«Антивирус и антишпион»** .
2. Откроется диалоговое окно настроек антивируса.
3. Нажмите вкладку «Устройства».
4. Выберите тип устройства, которое требуется настроить.
5. **Чтобы** отключить автозапуск для, снимите флажок **«Разрешить автоматическое выполнение файлов с этого устройства».**
6. **Чтобы** включить автозапуск для выбранного устройства, установите флажок **«Разрешить автоматическое выполнение файлов с этого устройства».**



Сканирование устройства

PRO32 Total Security позволяет сканировать съемные устройства при их подключении к системе.

Чтобы настроить сканирование съемного внешнего устройства при подключении:

1.Откройте стартовый экран продукта, затем **«Настройки защиты»** > , далее **«Настройки»** > модуля **«Антивирус и антишпион»** .

2. Откроется диалоговое окно настроек антивируса.

3. Нажмите вкладку «Устройства».
4. Выберите тип устройства, которое требуется настроить.
5. Выберите параметр **«Сканировать на вирусы, как только устройство будет подключено».** Это позволит сканировать устройство при его подключении.
6. При выборе параметра **«Запрашивать перед запуском сканирования будет предложено начать сканирование»** сразу после подключения устройства.
7. Выбор параметра «**Сканировать автоматически без отображения запроса»** позволит выполнять сканирование сразу после подключения устройства без каких-либо запросов.

5.6. Эвристика

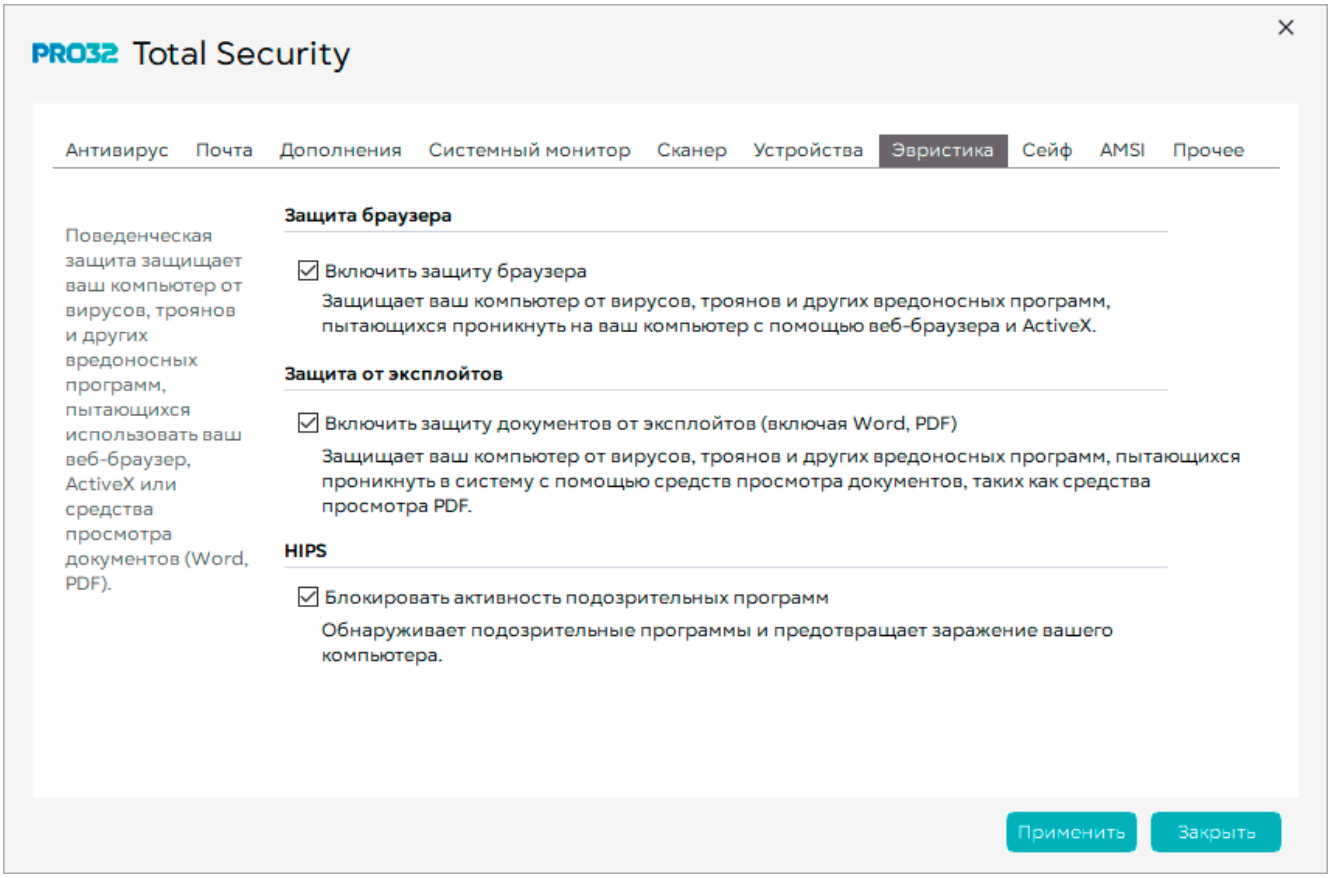
Защита браузера - (с применением новейших технологий Эвристики) позволяет обезопасить систему от вирусов, троянов и прочих угроз, которые могут проникать в систему с помощью веб-браузера, ActiveX и средства просмотра документов (PDF).

Защита от эксплойтов - обнаруживает и блокирует многие эксплойты браузера нулевого дня, включая автоматическую загрузку вредоносного ПО. Новый механизм упреждающей защиты,

который позволяет продукту обнаруживать и блокировать атаки нулевого дня с помощью эксплойтов на основе PDF.

HIPS - обнаруживает и блокирует подозрительные программы, чтобы не допустить повреждения вашей системы благодаря применению HIPS [хостовая система предотвращения вторжений]

1. Откройте стартовый экран продукта, затем **«Настройки защиты»** > , далее **«Настройки»** > модуля **«Антивирус и антишпион»** .
2. Откроется диалоговое окно настроек антивируса.
3. Нажмите вкладку «Эвристика».



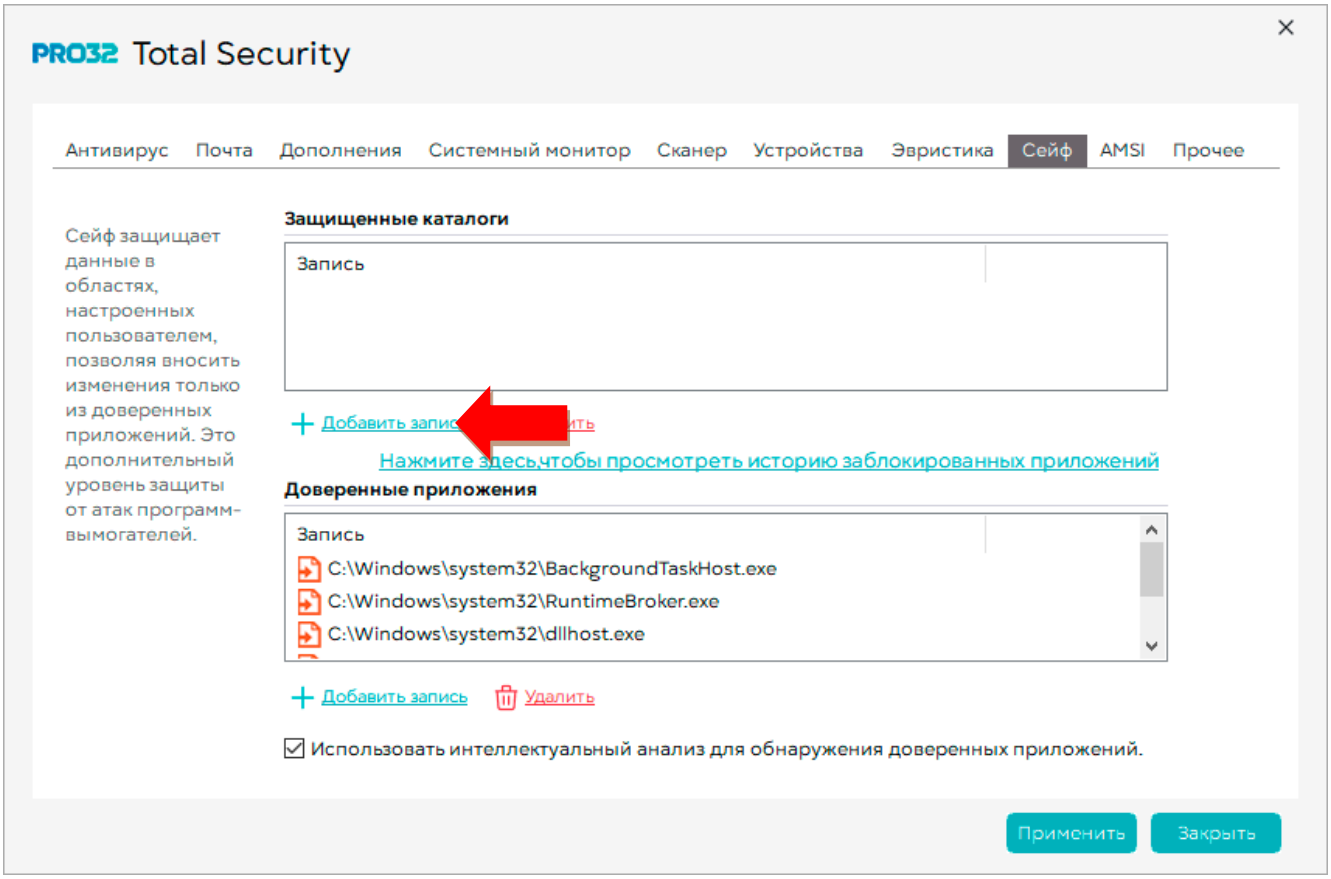
4. Установите или снимите значки с соответствующих параметров.

5.7. Сейф (защита от шифровальщиков)

Технология «Сейф» защищает данные в папках и подпапках от несанкционированного шифрования. Позволяет вносить изменения в папки (копирование, удаление, шифрование) только пользователям продукта PRO32 с помощью доверенных приложений. Это даёт дополнительный уровень защиты от программ-шифровальщиков.

Для настройки функции сейф:

1. Откройте стартовый экран продукта, затем **«Настройки защиты»** > , далее **«Настройки»** > модуля **«Антивирус и антишпион»** .
2. Откроется диалоговое окно настроек антивируса.
3. Нажмите вкладку «Сейф».
4. Для дополнительной защиты важных папок воспользуйтесь кнопкой «Добавить запись».



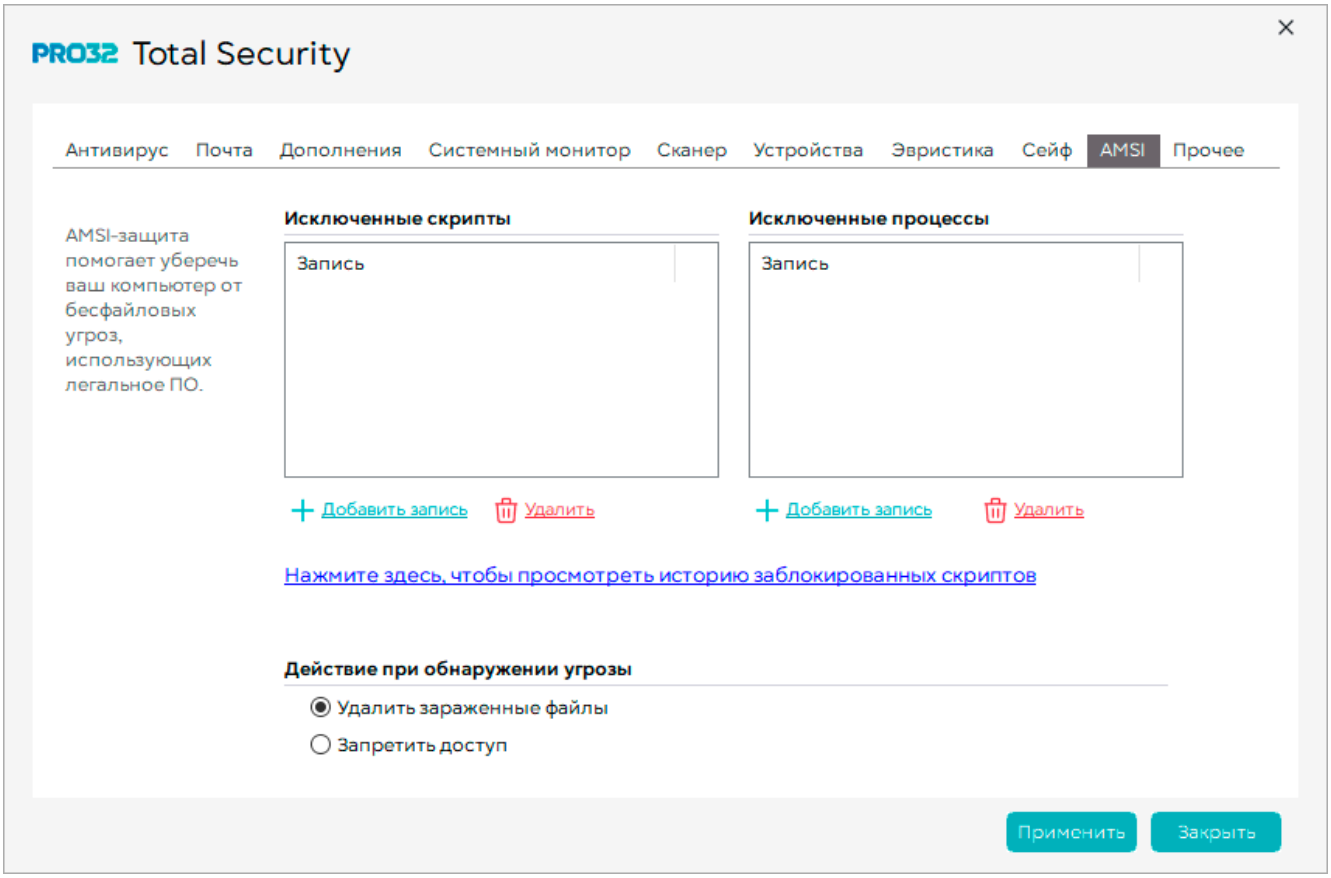
5. По умолчанию доступом к управлению файлами в добавленных вами папками и подпапками добавлены стандартные средства Windows. Если вы используете сторонние файловые менеджеры, вы можете добавить их в доверенные, воспользовавшись кнопкой **«Добавить запись»** + соответствующего раздела.

5.8. AMSI защита

AMSI (Anti Malware Scan Interface)– это интерфейс, используемый приложениями и службами в ОС Windows для отправки запросов на проверку в установленный на компьютере продукт для защиты от вредоносного ПО. Это обеспечивает дополнительную защиту от вредоносного ПО, которое использует сценарии или макросы в основных компонентах Windows, таких как PowerShell и Office365, или в других приложениях для предотвращения обнаружения.

Для настройки AMSI:

1. Откройте стартовый экран продукта, затем **«Настройки защиты»** >, далее **«Настройки»** модуля **«Антивирус и антишпион»**.
2. Откроется диалоговое окно настроек антивируса.
3. Нажмите вкладку **«AMSI».**
4. Вы можете исключить известные вам скрипты и процессы, воспользовавшись кнопкой **«Добавить запись»** +соответствующих разделов.
5. Вы можете посмотреть историю заблокированных скриптов в соответствующем разделе.



6. Так-же можно вы можете выбрать, что делать с обнаруженными угрозами – удалять или блокировать.

5.9. Настройка прочих параметров сканирования

PRO32 Total Security позволяет настраивать некоторые общие параметры сканирования.

Для настройки прочих параметров сканирования:

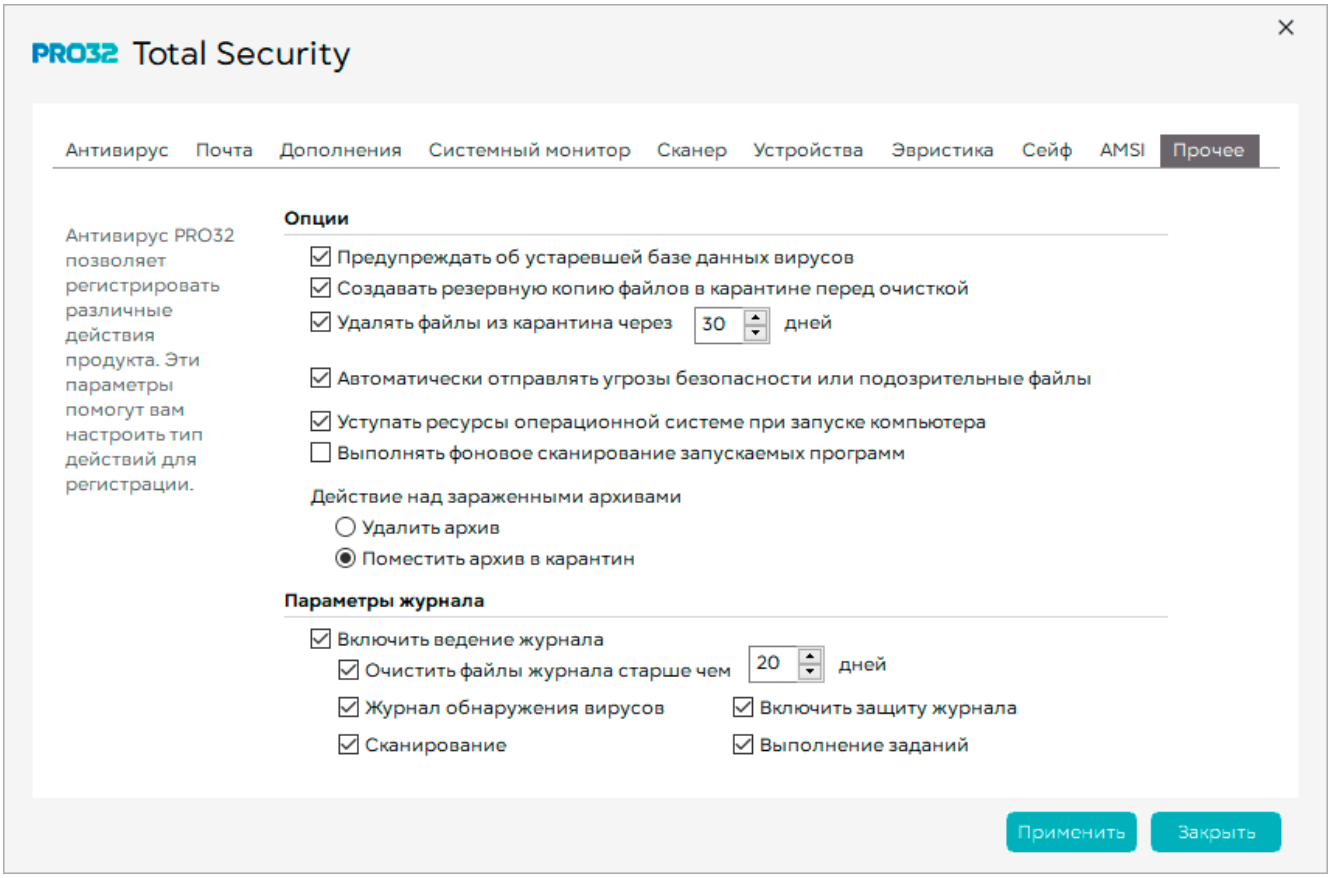
1. Откройте стартовый экран продукта, затем **«Настройки защиты»**, далее **«Настройки»** модуля **«Антивирус и антишпион»**.
2. Откроется диалоговое окно настроек антивируса.
3. Нажмите вкладку «Прочее».

Вкладка содержит следующие параметры:

Предупреждать об истечении срока действия базы данных с информацией о вирусах.
Отображает предупреждение, если определение вируса не обновлялось более 5 дней.

Создавать резервную копию файла в карантине перед очисткой
Создает копию карантинного файла в той же папке при выборе варианта очистки

Удалять файлы из карантина через «x» дней
Автоматически удаляет файлы, находящиеся в папке карантина, по истечении указанных «x» дней.



Включить контекстное меню в строке состояния

Отображает PRO32 Total Security в контекстном меню, вызываемом нажатием правой кнопкой мыши на значке PRO32 в области уведомлений.

Выполнять автоматические действия с зараженными архивами

Удалить архивы: если архив содержит один или несколько зараженных файлов, то он удаляется. Поместить архивы в карантин: если архив содержит один или несколько зараженных файлов, то он помещается в карантин

Автоматически отправлять угрозы безопасности или подозрительные файлы

Автоматически отправляет любые вредоносные файлы, на сервера PRO32 для их анализа. Выбор этого параметра позволяет вашему продукту участвовать в таких отправках.

Журнал обнаружения вирусов

Сохраняет сведения о вирусах, обнаруженных с помощью автоматического сканирования, сканера электронной почты, ручного сканирования, блокировки скриптов и блокировки червей, в отдельный файл

Удалять файлы журнала

Удаляет содержимое журнала, если он находился на вашем компьютере в течение старше «x» дней периода, превышающего 'x' дней.

Сканирование

Сохраняет сводку о результатах каждого сканирования, например, общее количество просканированных файлов, общее количество зараженных файлов и т.д., в отдельный файл.

Защита журнала

Записывает в журнал подробности, например, когда Sentry, системный монитор или защита электронной почты Вкл./Выкл. отключается или включается.

Завершенные задачи

Сохраняет сведения о завершенных задачах сканирования в файл.

4. Нажмите кнопку **«Применить»** для сохранения настроек.

6. Управление файлами в карантине

Функция карантина позволяет временно изолировать зараженные и подозрительные файлы в папку карантина до тех пор, пока не будут предприняты соответствующие действия. Файлы, перемещенные в папку карантина, могут содержать вирус или вредоносную программу. Обновите свое приложение PRO32 Total Security и очистите компьютер, прежде чем восстановить помещенный в карантин файл в его исходное местоположение.

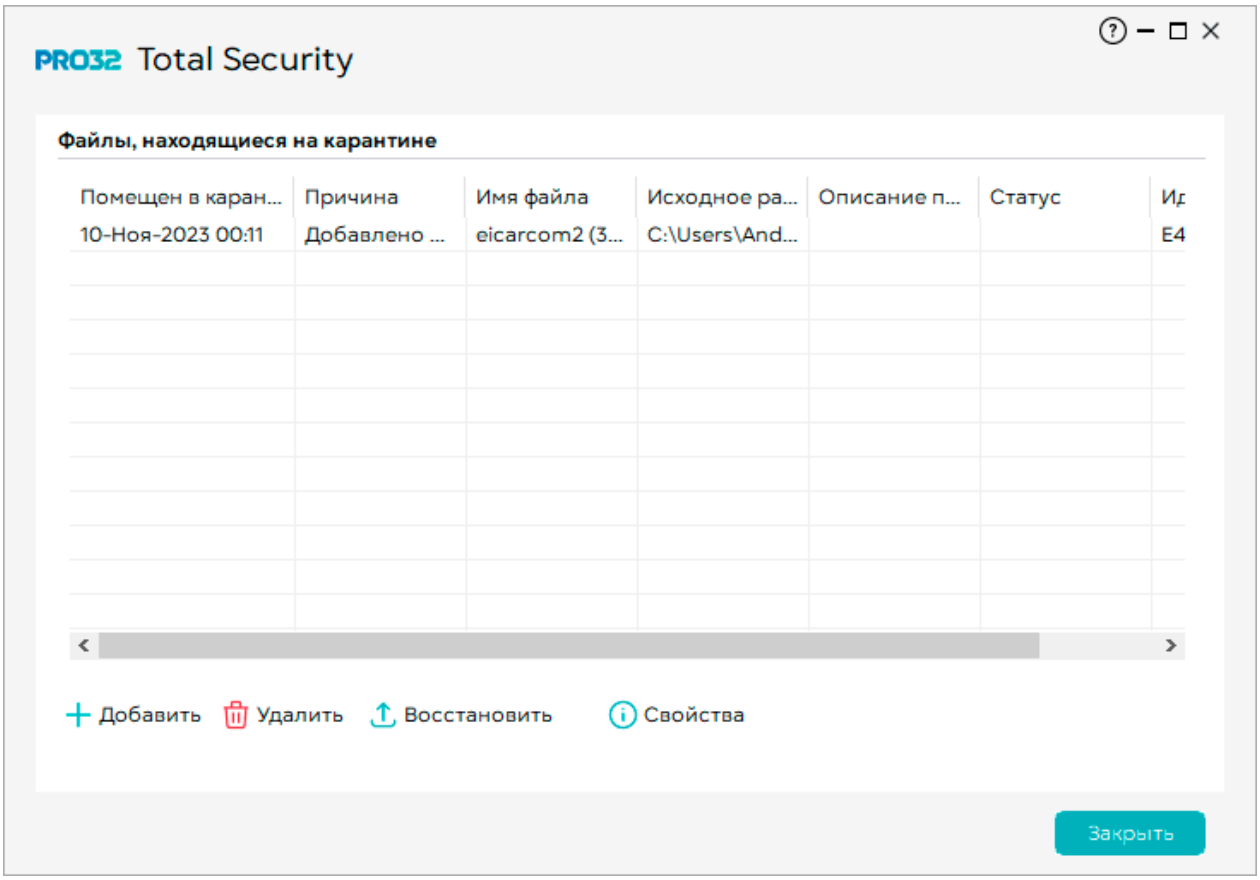
Управление файлами в карантине:

Откройте стартовый экран продукта ⌂, затем **«Настройки защиты»** ›, далее **«Карантин»** ›
Откроется консоль диспетчера карантина.

В консоли отображается список объектов, помещенных в карантин. Для каждого файла отображаются такие сведения, как имя файла, исходное местоположение, дата помещения в карантин, описание проблемы, статус и идентификатор файла.

Вы можете выбрать одно из следующих действий:
- Добавление файлов в папку карантина
- Удаление файлов в карантине
- Восстановление файлов из карантина в их исходные местоположения

Для получения дополнительных сведений о файле, помещенном в карантин, и его текущем состоянии, выберите файл в списке и нажмите Свойства.
Нажмите **«Закрыть»** для закрытия консоли диспетчера карантина.



6.1. Добавление файлов в папку карантина

Если вы подозреваете, что файл заражен, то можете вручную добавить его в папку карантина.

1. Откройте стартовый экран продукта, затем **«Настройки защиты»** > **,** далее **«Карантин»** > Откроется консоль диспетчера карантина.
2. Нажмите **«Добавить»** +. Откроется диалоговое окно **«Добавить файлы в карантин».**
3. Выберите файл, который требуется добавить в папку карантина, и нажмите **«Открыть».**

*Примечание: чтобы удалить файл из этого места, выберите **«Восстановить»** из этого местоположения в диалоговом окне «Добавить файлы в карантин».

4. Файл будет добавлен в папку карантина и указан в диалоговом окне.
5. Вы можете выполнить действия с файлом позже.
6. Нажмите кнопку, **«Закрыть»** чтобы закрыть консоль диспетчера карантина.

6.2. Восстановление файлов из карантина

Вы можете восстановить файлы из карантина в их исходные местоположения. Если вы заподозрили системный файл и переместили его в папку карантина, соответствующая программа может работать некорректно. В таком случае вам нужно будет переместить файл обратно в исходное место, чтобы соответствующая программа работала правильно.

*Важно: перед восстановлением помещенного в карантин файла загрузите обновления продукта, запустите сканирование и очистите файл.

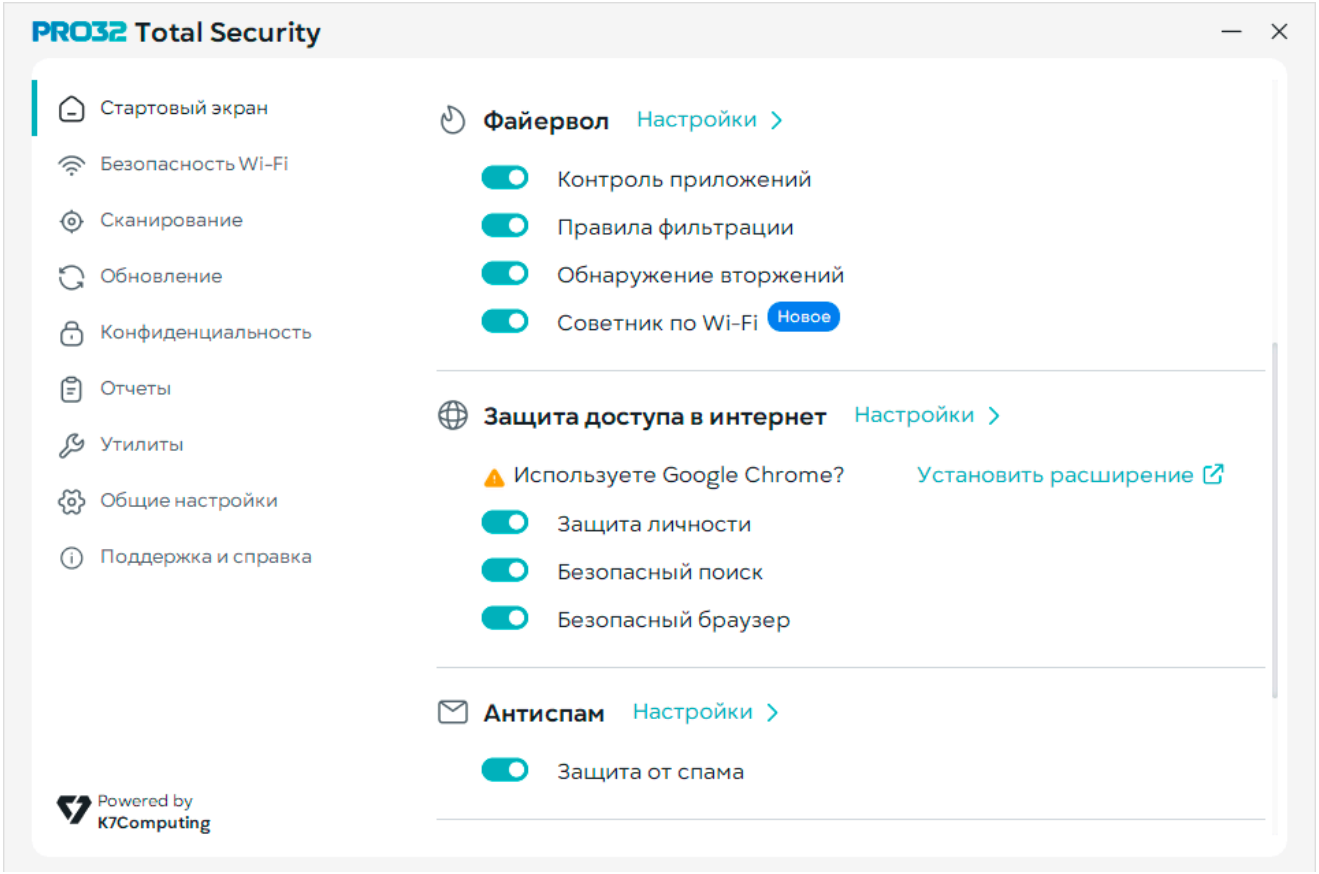
Для восстановления файлов из карантина:

1. Откройте стартовый экран продукта, затем **«Настройки защиты»** > **,** далее **«Карантин»** > или воспользуйтесь боковой панелью **«Отчёты»** слева. Откроется консоль диспетчера карантина.
2. Выберите файл, который требуется восстановить, и нажмите **«Восстановить».** Появится предупреждающее сообщение о восстановлении помещенного в карантин файла.
3. Нажмите **«Да»,** если хотите восстановить файл. Файл будет возвращен в исходное место.
6. Нажмите кнопку, **«Закрыть»** чтобы закрыть консоль диспетчера карантина.

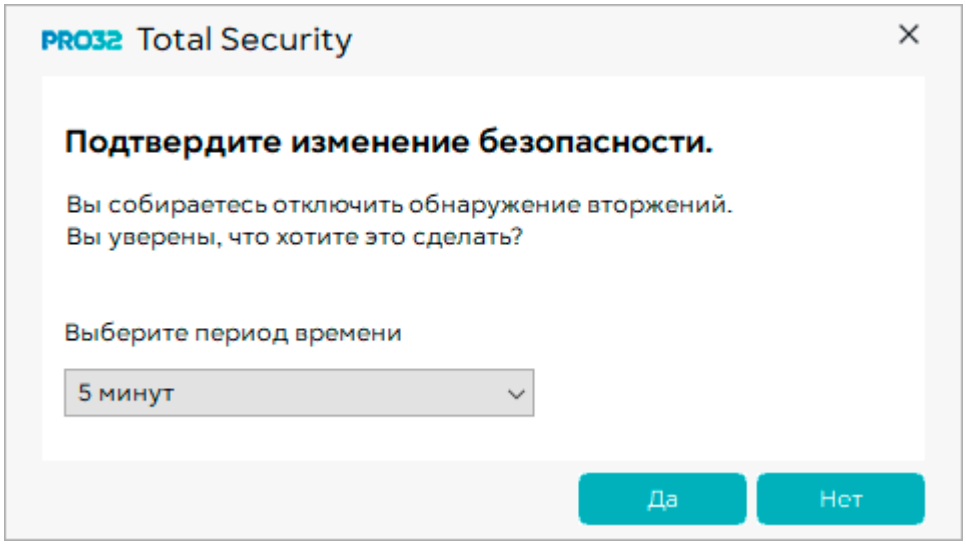
7. Модуль «Файерволл» (Брандмауер)

Брандмауэр PRO32 защищает ваш компьютер от вторжений, нежелательных подключений, сканирования портов и хакерских атак. Он блокирует любые программы, которые пытаются получить доступ к Интернету, кроме тех, которые настроены вами как доверенные. Брандмауэр PRO32 обеспечивает упреждающую защиту для предотвращения входящих, исходящих и программных атак и делает ваш компьютер полностью невидимым для хакеров. Он предотвращает отправку личной информации через Интернет шпионскими и другими вредоносными программами.

Когда брандмауэр PRO32 включен, он действует как барьер между вашим компьютером и Интернетом, незаметно отслеживая интернет-трафик, поступающий на ваш компьютер, на предмет подозрительной активности, а также предупреждая вас о потенциальных угрозах.



Состояние функций изображается выключателями . По умолчанию все компоненты и модули продукта включены и имеют преднастроенные правила работы. Для того, чтобы быстро отключить какой-либо модуль, переключите выключатель в состояние «Выкл» .



Выберите время, на которое хотите отключить тот или иной модуль и подтвердите выбор кнопкой **«Да».**

Модуль «Файерволл» содержит в себе 4 выключателя для быстрого доступа:

Контроль приложений

Настроив управление доступом к приложениям, вы можете контролировать, каким программам на вашем компьютере разрешен доступ в Интернет. По умолчанию брандмауэр PRO32 автоматически добавляет в список программы, которые считает безопасными. Когда программа, которой нет в списке, попытается получить доступ к Интернету, вы получите уведомление. Вы

можете разрешить или заблокировать доступ в Интернет для соответствующей программы.

Правила фильтрации

Можно создавать правила для каждого приложения, которое получает доступ к Интернету, чтобы контролировать его поведение. Вы можете редактировать существующие правила и создавать собственные

Обнаружение вторжений

Функция обнаружения вторжений сканирует весь входящий сетевой трафик и сравнивает эту информацию с данными об атаках. Это позволяет выявлять попытки злоумышленников скомпрометировать вашу систему. Это защитит вашу систему от распространенных интернет-атак.

Советник по Wi-Fi

PRO32 постоянно ведёт мониторинг опасных общедоступных Wi-Fi точек. При подключении к такой, продукт даст оповещение об угрозах и предложит оптимальные настройки безопасного подключения к такой точке.

7.1. Настройка правил подключения к сети

Для управления брандмауэром (файерволлом):

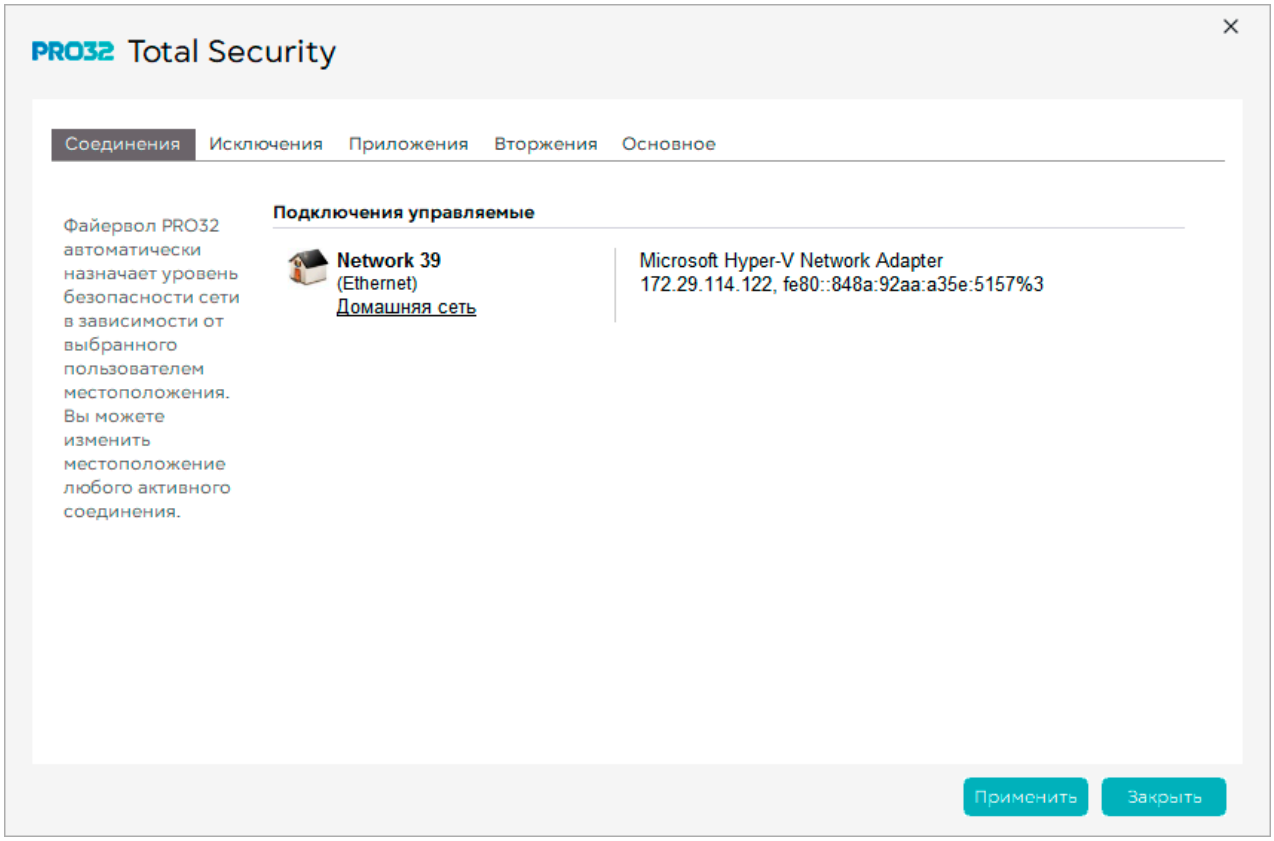
1. Откройте стартовый экран продукта, затем **«Настройки защиты»** > , далее **«Настройки»** > модуля **«Файерволл»** .
2. Откроется диалоговое окно настроек Файерволла.

Брандмауэр PRO32 защищает вашу систему на основе правил. Этот набор правил зависит от выбранного сетевого профиля. При первом подключении системы к какой-либо сети вам нужно будет выбрать сетевое расположение. Это позволит автоматически установить соответствующие правила брандмауэра/профиль и уровень безопасности. Если вы подключаете свою систему в разных местах, например дома, на работе, в кафе или в аэропорту, правильный выбор расположения обеспечит надлежащую защиту вашей системы.

Существует три варианта сетевого расположения, которые будут автоматически предложены для выбора при обнаружении новой сети:

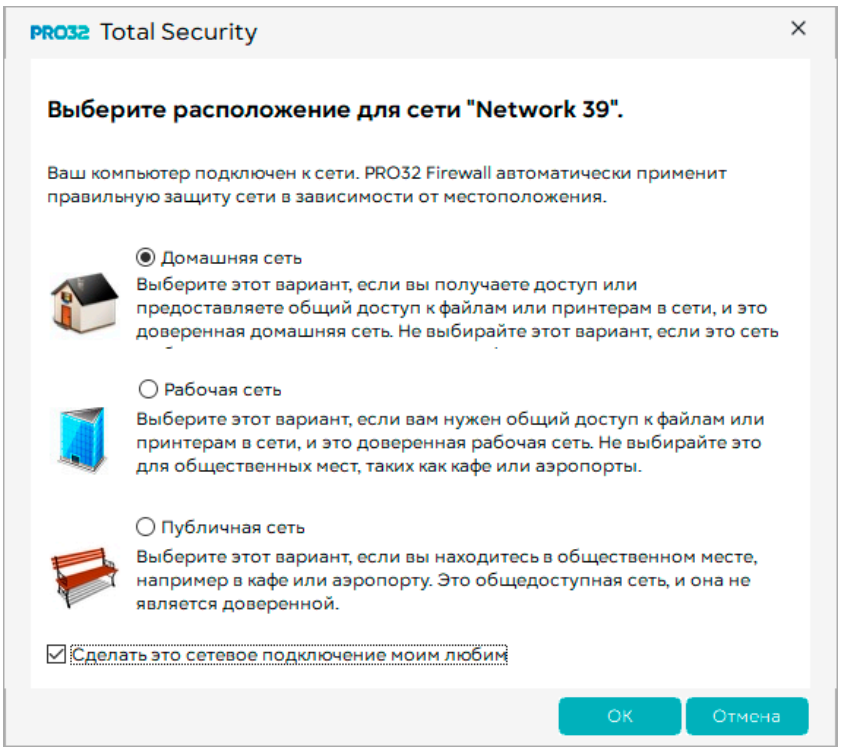
Домашняя сеть – выберите это расположение, если вы подключаетесь из своей домашней сети или из любой другой сети, которую вы знаете и можете доверять другим людям или устройствам из этой сети. Это позволяет вам видеть другие компьютеры и устройства в сети, а также дает возможность другим пользователям сети видеть ваш компьютер.

Рабочая сеть – выберите этот вариант, если вы подключаетесь к офисной сети или к сети на другом рабочем месте. Это позволяет вам видеть другие компьютеры и устройства в сети, а также дает возможность другим пользователям сети видеть ваш компьютер. Однако система не сможет присоединиться к сети.



Публичная сеть – выберите этот вариант, если вы находитесь в общественном месте, например, в кафе или аэропорту. При этом ваша система не будет видимой для других компьютеров, подключенных к сети, что обеспечит защиту от интернет-атак при подключении через общедоступную сеть.

*Рекомендуется всегда выбирать местоположение «Общедоступная сеть», когда вы находитесь в общественном месте, например, в кафе или в аэропорту. Для этого установите флажок напротив опции **«Сделать это сетевое подключение моим любимым»**

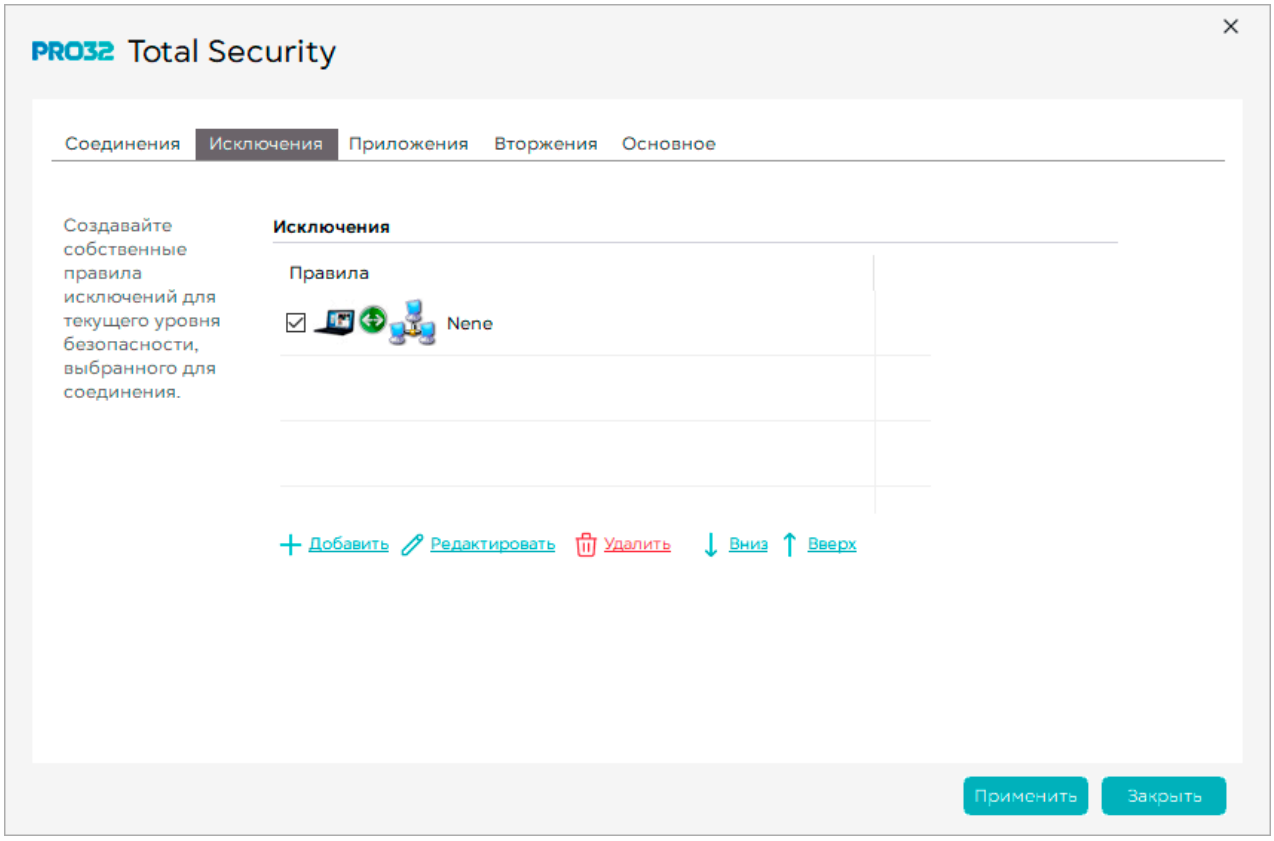


7.2. Настройка правил файерволла для приложений

Настроив управление доступом к приложениям, вы можете контролировать, каким программам на вашем компьютере разрешен доступ в Интернет. По умолчанию брандмауэр PRO32 автоматически добавляет в список программы, которые считает безопасными. Когда программа, которой нет в списке, попытается получить доступ к Интернету, вы получите уведомление. Вы можете разрешить или заблокировать доступ в Интернет для соответствующей программы.

1.Откройте стартовый экран продукта , затем **«Настройки защиты»** , далее **«Настройки»** модуля **«Файерволл»** .
2. Откроется диалоговое окно настроек Файерволла.

3. Откройте вкладку **«Исключения»**

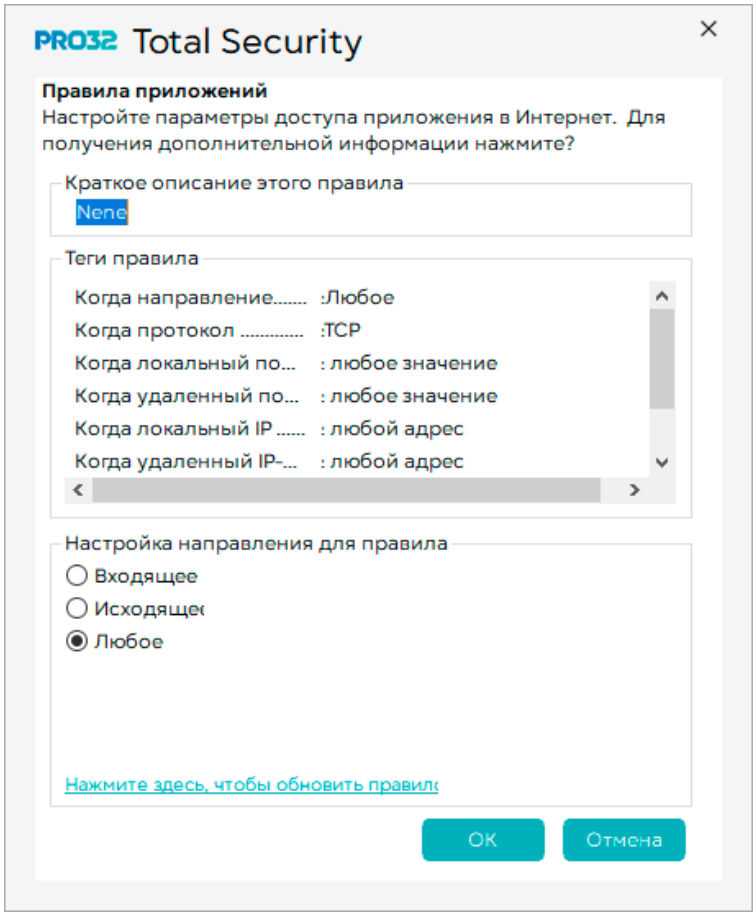


Выберите **Метку правила** и настройте ее свойства на нижней панели. Параметры, отображаемые на нижней панели, зависят от выбранной метки.

В следующей таблице описаны параметры, доступные для каждой метки правила:

Метка правила	Что нужно настроить	Параметр	Описание
Когда направление	**Направление**	**Входящее**	Правило распространяется на входящие подключения с других компьютеров к вашему компьютеру
		Исходящее	Правило распространяется на исходящие подключения других компьютеров к вашему компьютеру

		Оба варианта	Правило применяется как к входящим, так и к исходящим соединениям
Когда протокол	**Протокол**	**Любой протокол**	Правило распространяется на любой обмен данными
		TCP	Правило применяется к обмену данными по протоколу TCP (Transmission Control Protocol)
		UDP	Правило применяется к обмену данными по протоколу UDP (User Data gram Protocol)
		TCP или UDP	Правило применяется к обмену данными по протоколам TCP и UDP
	Конкретный протокол		Правило применяется к указанному здесь протоколу
Когда локальный порт	**Любой адрес порта**		Правило применяется к обмену данными, исходящему от локального компьютера, с использованием любого порта
	Адрес конкретного порта		Правило применяется к обмену данными, исходящему от локального компьютера, с использованием указанного здесь порта
	Диапазон адресов портов		Правило применяется к обмену данными исходящему от локального компьютера, с использованием указанного здесь диапазона портов
Когда удаленный порт	**Любой адрес порта**		Правило применяется к обмену данными, исходящему от другого компьютера, с использованием любого порта



Тег правила	Что нужно настроить	Параметр	Описание
		Адрес конкретного порта	Правило применяется к обмену данными, исходящему от другого компьютера, с использованием указанного здесь порта
		Диапазон адресов портов	Правило применяется к обмену данными, исходящему от другого компьютера, с использованием указанного здесь диапазона портов
Если локальный IP-адрес	**Исходный IP-адрес**	**Любой IP-адрес**	Правило применяется к обмену данными, исходящему с любого локального IP-адреса
		Конкретный IP-адрес	Правило применяется к обмену данными, исходящему с указанного здесь локального IP-адреса
		Диапазон IP-адресов	Правило применяется к обмену данными, исходящему с локального IP-адреса, который попадает в указанный

			диапазон IP-адресов.
		Сетевой адрес	Правило применяется к обмену данными, исходящему с локального IP-адреса, который попадает в указанную сеть
Если удаленный IP-адрес	**Удаленный IP-адрес**	**Любой IP-адрес**	Правило распространяется на обмен данными с использованием любого IP-адреса
		Конкретный IP-адрес	Правило применяется к обмену данными на указанный здесь удаленный IP-адрес
		Диапазон IP-адресов	Правило применяется к обмену данными на удаленный IP-адрес, который попадает в указанный диапазон IP-адресов.
		Сетевой адрес	Правило применяется к обмену данными на удаленный IP-адрес, который попадает в указанную сеть
Действие	**Действие, выполняемое правилом**	**Разрешить пакет**	Разрешает обмен данными, который соответствует настроенному правилу
		Блокировать пакет	Блокирует обмен данными, который соответствует настроенному правилу
		Показать уведомление	Отображает уведомление, когда обмен данными соответствует этому правилу
		Создать запись журнала	Создает запись в журнале, когда обмен данными соответствует этому правилу

2. В случае настройки правила нажмите пункт **Обновить**, чтобы сохранить изменения в правиле.

3. Нажмите **ОК** для закрытия диалогового окна **«Определение правила».**

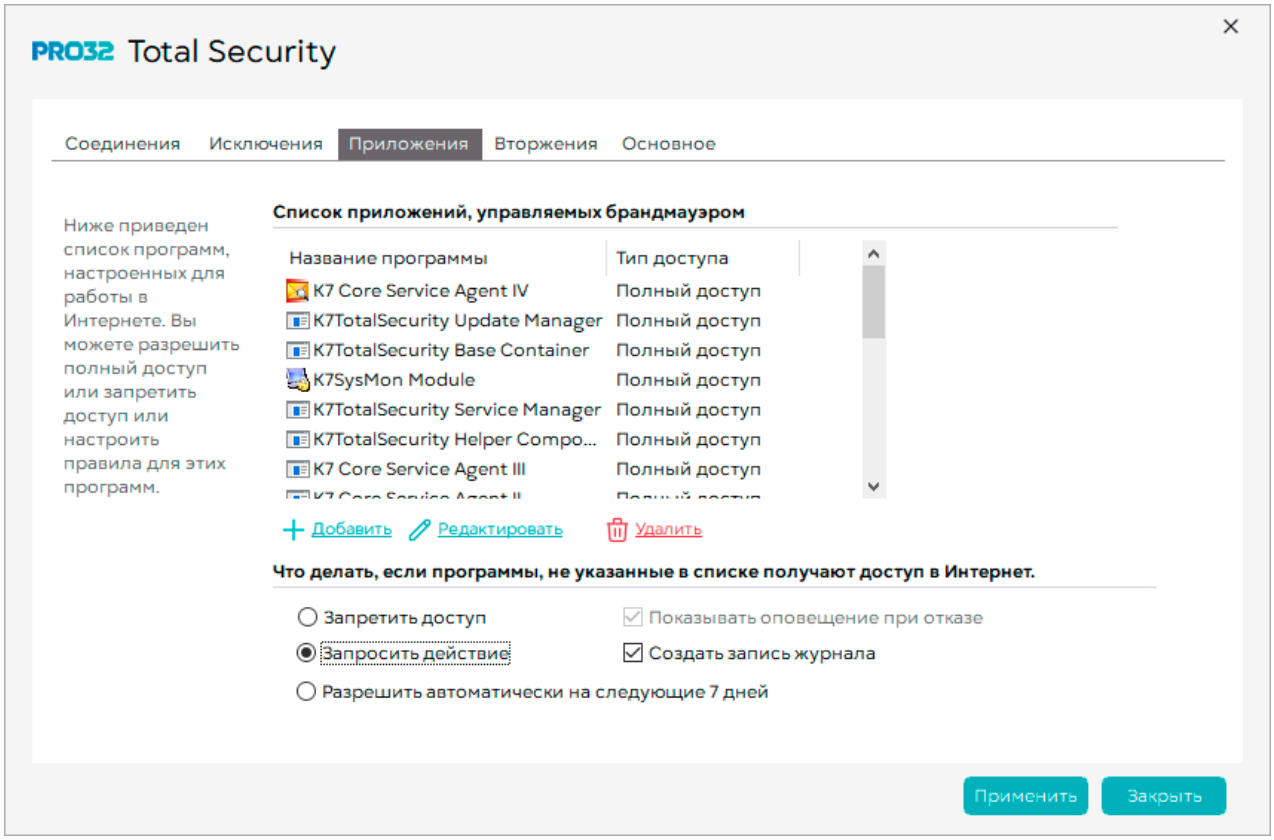
4. Для редактирования созданного правила нажмите кнопку «Редактировать» 

7.3. Настройка правил файерволла для приложений, имеющих доступ в сеть Интернет

1. Откройте стартовый экран продукта , затем **«Настройки защиты»** , далее **«Настройки»** модуля **«Файерволл»** .

2. Откроется диалоговое окно настроек Файерволла.

3. Откройте вкладку **«Приложения»**



4. Будет показан список приложений с соответствующими разрешениями на доступ в Интернет.

5. Вы можете предпринять одно из следующих действий:

- Добавить приложение в список
- Изменить правила для приложения
- Удалить приложение из списка

6. Укажите действие, которое будет выполняться при доступе к Интернету программ, не включенных в список, на панели **«Что делать»,** если программы, неуказанные в списке выше, получают доступ в Интернет.

Запретить доступ - Блокирует доступ для всех приложений, которые отсутствуют в списке приложений. Флажок **«Показывать оповещение при отказе»** становится активным при выборе этого параметра.

Запрашивать действие - Запрашивает разрешение на доступ при попытке нового приложения получить доступ к Интернету. Вы можете разрешить или заблокировать доступ в Интернет для приложения.

Показывать оповещение при отказе - Отображает оповещение, когда приложению будет отказано в доступе к Интернету. Этот параметр активируется при выборе варианта Запретить доступ.

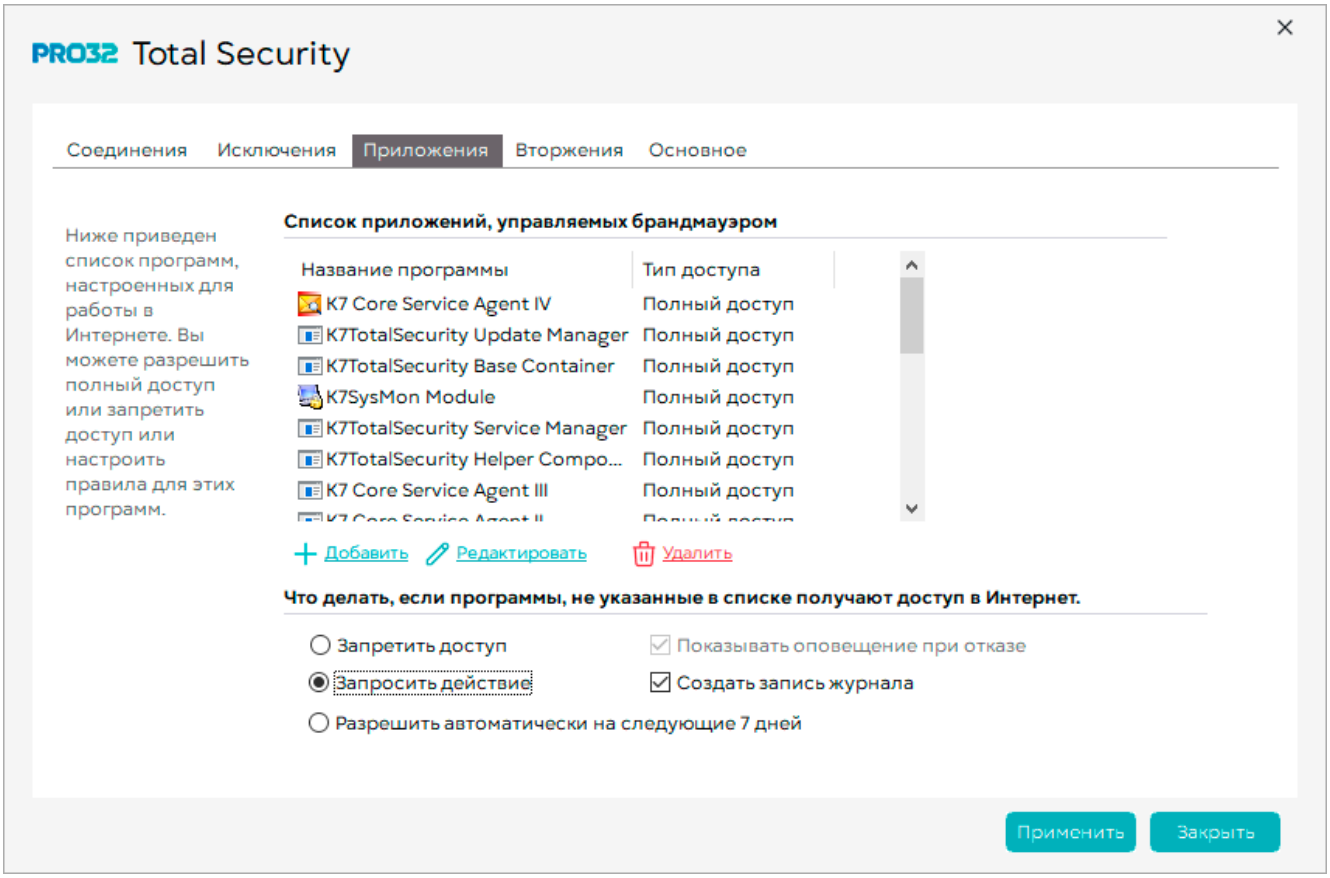
Флажок **«Создать запись журнала»** - Создает запись в журнале, когда новое приложение получает доступ к Интернету.

Разрешить автоматически в течение следующих 7 дней - Этот вариант автоматически добавит приложение, имеющее доступ к Интернету, в список разрешенных приложений брандмауэра в течение первых 6 дней после установки продукта. Это означает, что продукт будет находиться в режиме обучения в течение первых 6 дней.

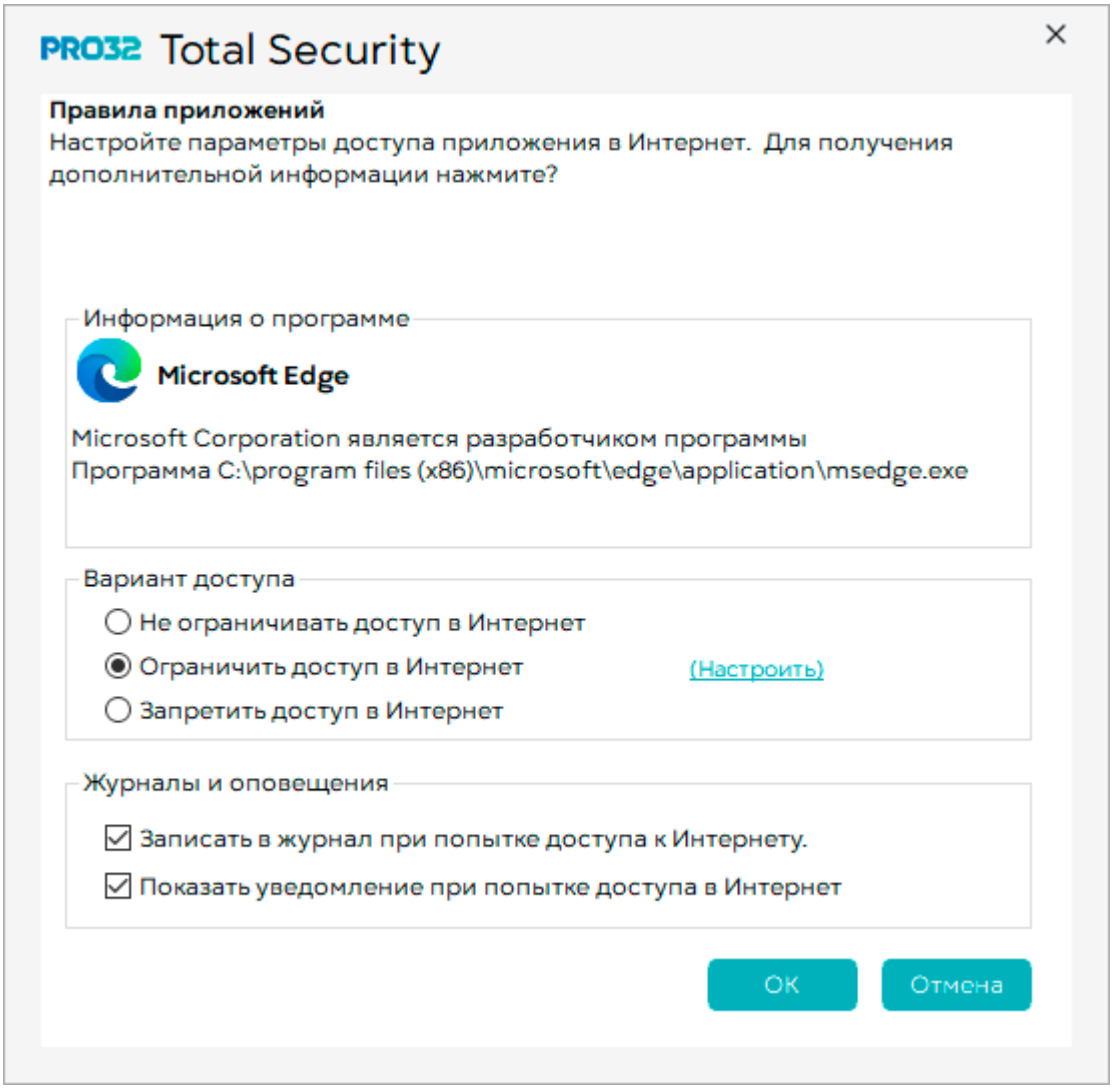
7.4. Добавление приложения в список управления доступом

Вы можете добавить приложения и настроить права доступа в Интернет для этих приложений. Вы можете предоставить полный доступ, ограниченный доступ либо же запретить доступ для приложений.

1.Откройте стартовый экран продукта , затем **«Настройки защиты»**, далее **«Настройки»** модуля **«Файерволл»** .
2. Откроется диалоговое окно настроек Файерволла.
3. Откройте вкладку **«Приложения».**
4. Выберите из уже преднастроенных приложений или добавьте необходимое нажав кнопку **«Добавить»** +



5. Затем, нажмите кнопку **«Редактировать»** Установите соответствующий флажок, чтобы установить параметры **журнала и уведомлений** для **приложения**. Параметры описаны в следующей таблице.



Параметр	Описание
Программа имеет неограниченный доступ в Интернет	Разрешает приложению осуществлять полный доступ к Интернету
Программа имеет ограниченный доступ в Интернет	Разрешает приложению доступ в Интернет на основе набора правил
Не разрешать программе доступ в Интернет	Блокирует доступ приложения в Интернет

6. Установите\снимите соответствующий флажок, чтобы установить параметры журнала и уведомлений для приложения. Параметры описаны в следующей таблице.

Действие	Описание
Создавать запись журнала всякий раз, когда эта программа получает доступ к Интернету	Регистрирует все действия, когда приложение выходит в Интернет
Отображать оповещение всякий раз, когда эта программа получает доступ к Интернету	Отображает оповещение всякий раз, когда программа получает доступ к Интернету

7. Нажмите **«ОК»** для сохранения настроек. Приложение будет добавлено в список контроля доступа и появится в списке приложений.

7.5. Удаление приложения из списка управления доступом

Чтобы удалить приложение из списка контроля доступа:

1. Откройте стартовый экран продукта, затем **«Настройки защиты»** > , далее **«Настройки»** > модуля **«Файерволл»** .
2. Откроется диалоговое окно настроек Файерволла.
3. Откройте вкладку **«Приложения».**
4. Выберите из настроенное приложение, затем удалите настройки нажав кнопку **«Удалить»**

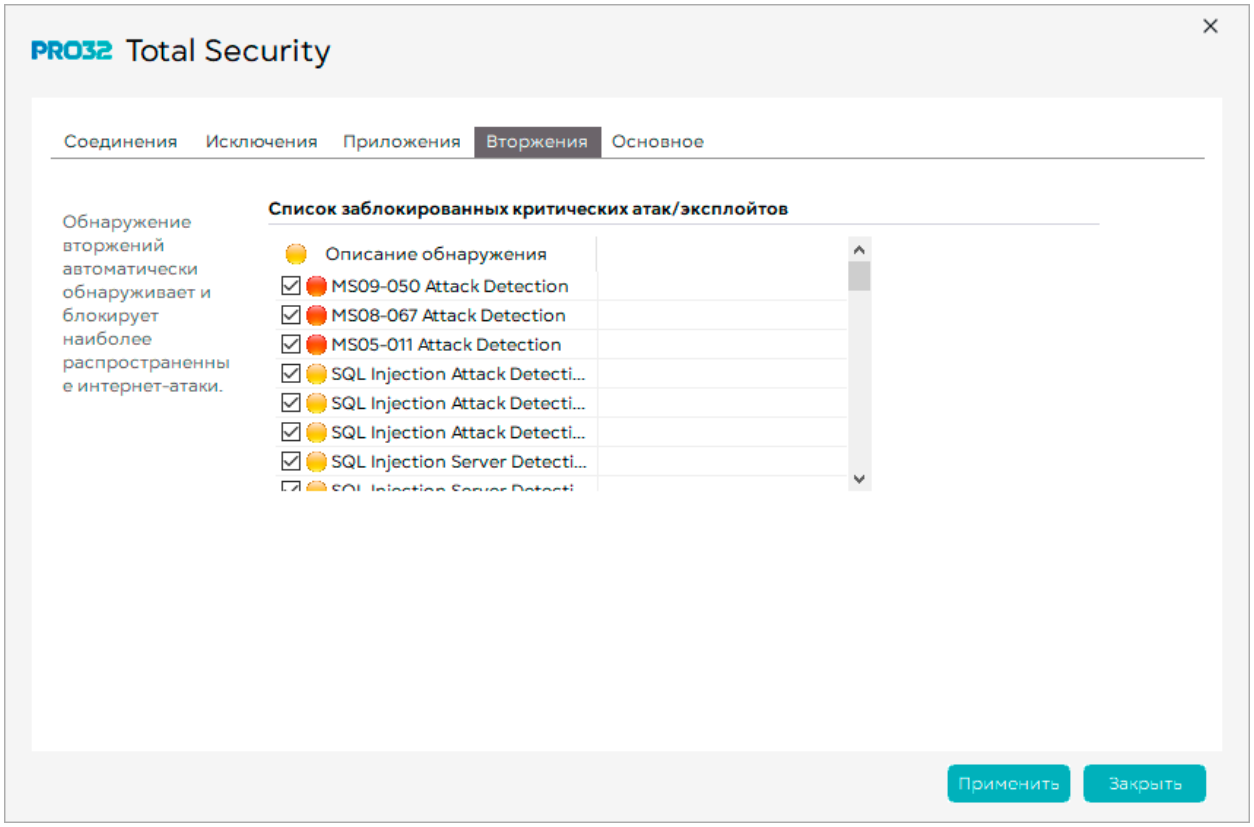
7.6. Обнаружение вторжений

Функция обнаружения вторжений сканирует весь входящий сетевой трафик и сравнивает эту информацию с данными об атаках. Это позволяет выявлять попытки злоумышленников скомпрометировать вашу систему. Это защитит вашу систему от распространенных интернет-атак.

В некоторых сценариях законная сетевая активность может совпадать с определениями атаки. В этом случае будут возникать множественные сообщения о возможных атаках. Если вы уверены, что эти сетевые действия безопасны, вы можете отключить эти определения.

1. Откройте стартовый экран продукта, затем **«Настройки защиты»**, далее **«Настройки»** модуля **«Файерволл»** .
2. Откроется диалоговое окно настроек Файерволла.
3. Откройте вкладку **«Вторжения».**
4. В списке заблокированных атак / эксплойтов снимите флажки тех позиций, которые требуется исключить.
5. Нажмите **«Применить»,** чтобы эти изменения вступили в силу.

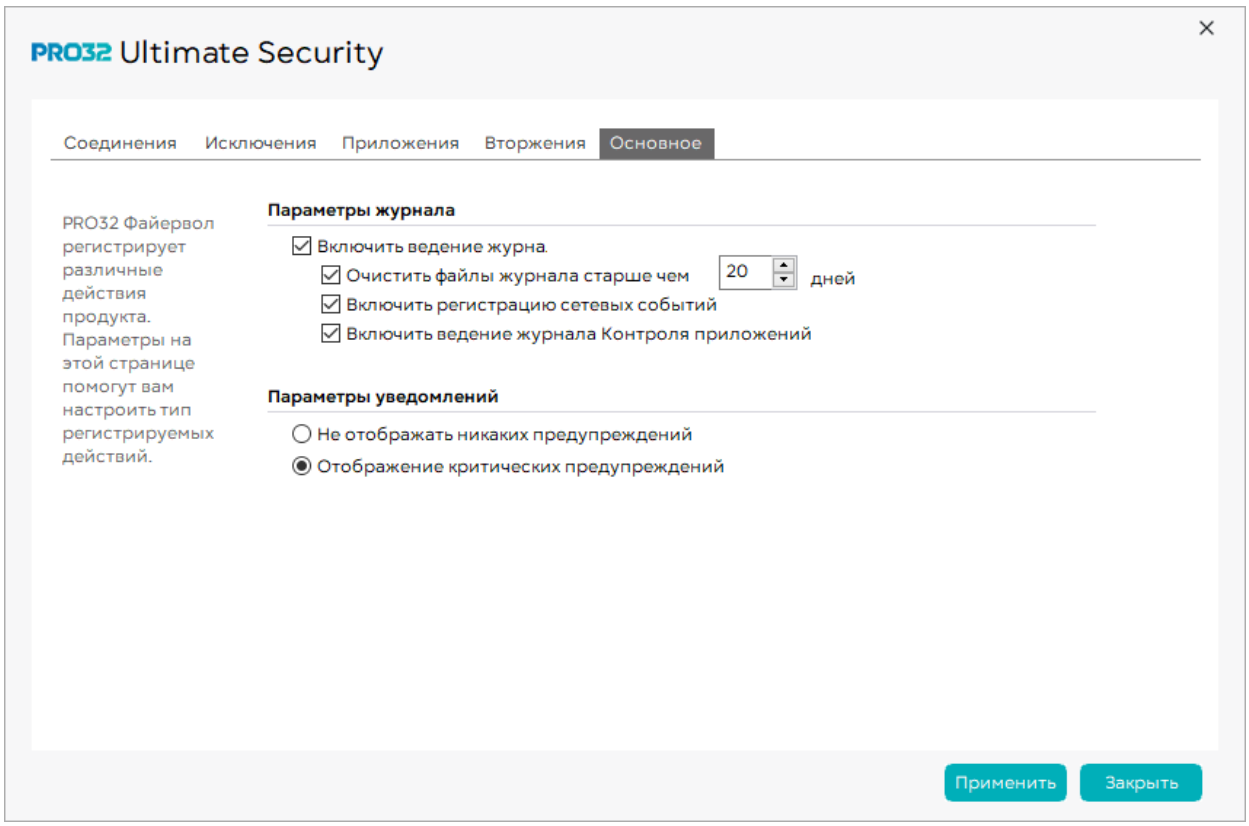
*Примечание: не рекомендуется исключать какие-либо определения атак, поскольку это может сделать вашу систему уязвимой для атак.



2.7. Настройка общих параметров брандмауэра

Брандмауэр PRO32 позволяет настраивать некоторые общие параметры, например, параметры журнала и предупреждений.

1. Откройте стартовый экран продукта, затем **«Настройки защиты»** > , далее **«Настройки»** > модуля **«Файерволл»** .
2. Откроется диалоговое окно настроек Файерволла. Откройте вкладку **«Основное».**



3. Параметры описаны в следующей таблице:

Параметр	Описание
Включить ведение журнала	Выберите эту опцию, если хотите, чтобы брандмауэр PRO32 регистрировал действия в журнале
Очистить файлы журнала старше «x» дней	Удаляет содержимое журнала возрастом более «x» дней
Включить регистрацию сетевых событий	Регистрирует сведения о трафике, заблокированном с применением правил брандмауэра.
Включить ведение журнала доступа к приложению	Регистрирует сведения о трафике, заблокированном с применением контроля доступа к приложениям.

3. Выбрать «**Параметры уведомлений»**. Параметры описаны в следующей таблице:

Параметр	Описание
Не отображать оповещения	Оповещения брандмауэра PRO32 отображаться не будут
Отображать оповещения	Отображает оповещение в случае блокировки трафика

8. Модуль «Защита доступа в Интернет»

Состояние функций модуля изображается выключателями . По умолчанию все компоненты и модули продукта включены и имеют преднастроенные правила работы. Для того, чтобы быстро отключить какой-либо модуль, переключите выключатель в состояние «Выкл» .

Выберите время, на которое хотите отключить тот или иной модуль и подтвердите выбор кнопкой **«Да».**

Защита в интернете включает в себя следующее:

Безопасный просмотр сайтов: обеспечивает защиту от веб-сайтов, которые могут нанести вред вашему компьютеру и похитить вашу конфиденциальную информацию

Безопасный поиск: улучшает результаты поиска в Интернете за счет размещения индикаторов доверия (подписей к значкам) рядом с выводимыми результатами.

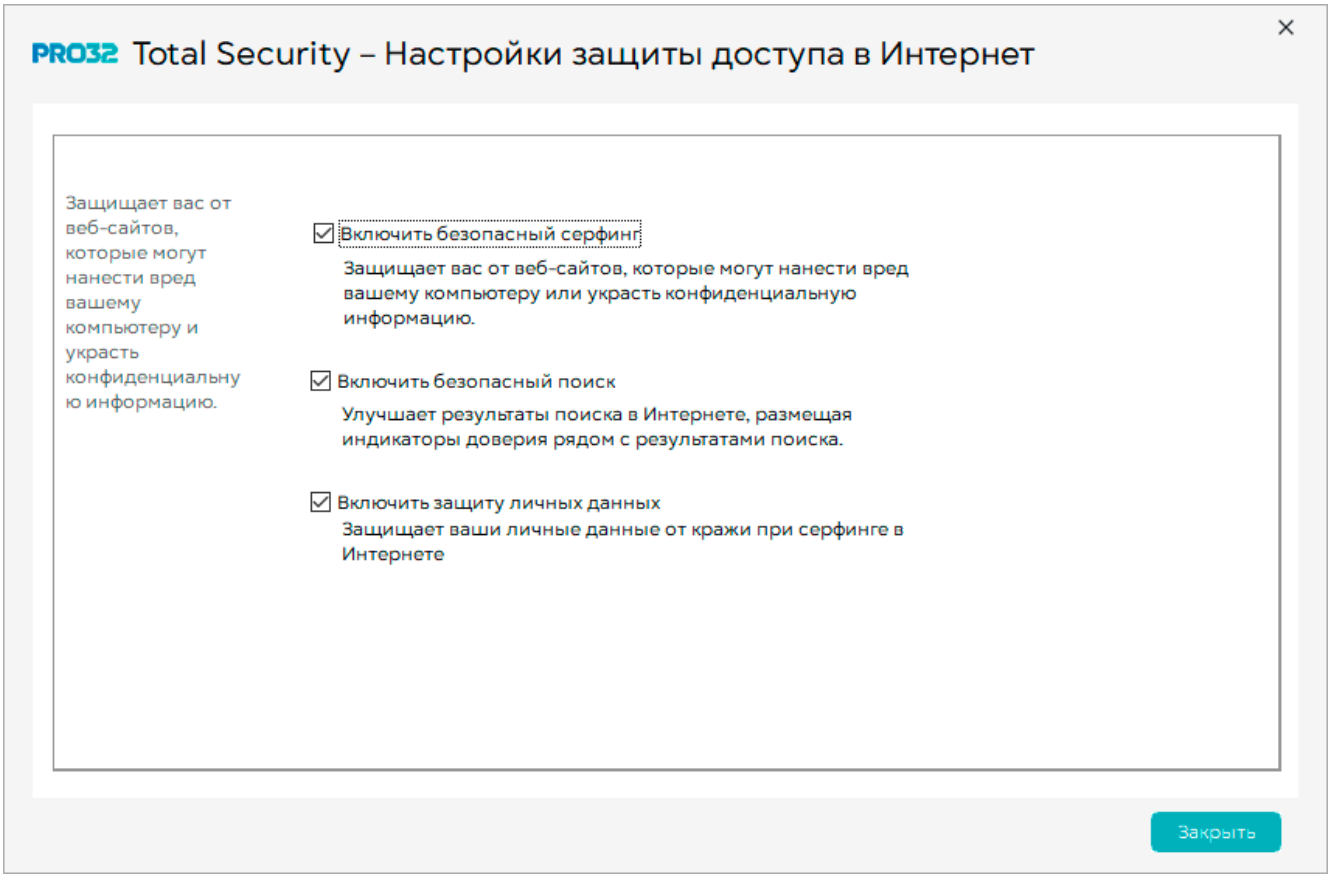
Защита личных данных: защищает ваши личные данные от кражи при просмотре веб-страниц, отображая оповещение при вводе паролей на сайтах, которые не используют протокол https.

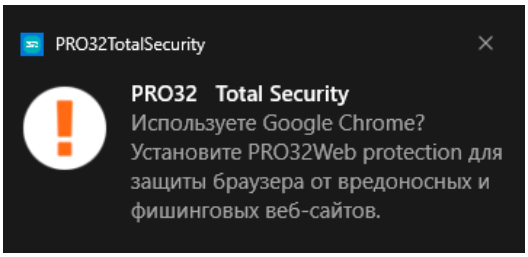
По умолчанию все три функции будут включены при установке продукта.

Для отключения любой из этих функций:

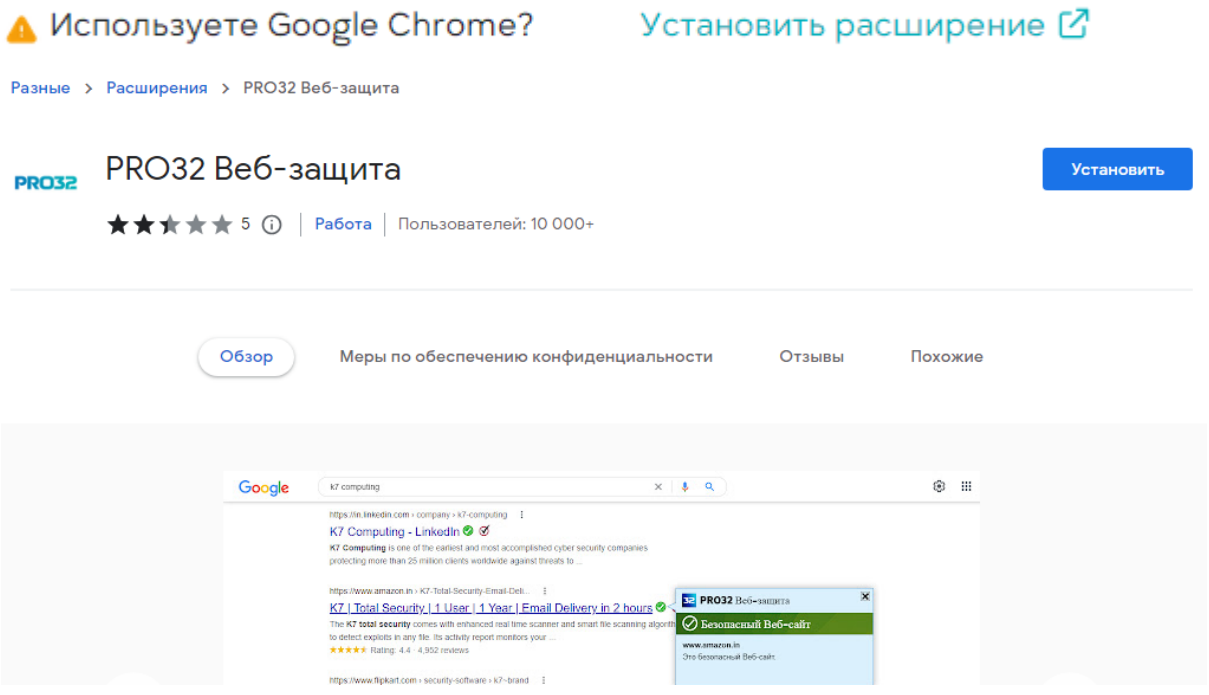
1. Откройте стартовый экран продукта , затем **«Настройки защиты»** , далее **«Настройки»** модуля **«Защита доступа в Интернет»** .

2. Откроется диалоговое окно настроек модуля **«Защита доступа в Интернет».**





Аннотации значков безопасного поиска отображаются в Google, Yahoo и Bing при использовании с браузерами Internet Explorer, Firefox и Chrome. Для этого требуется установить отдельный плагин для браузера. Дождитесь всплывающего окна антивируса и следуйте инструкции.



*Защита личных данных работает только в Internet Explorer и Firefox.

Настройка блокировки вредоносных сайтов

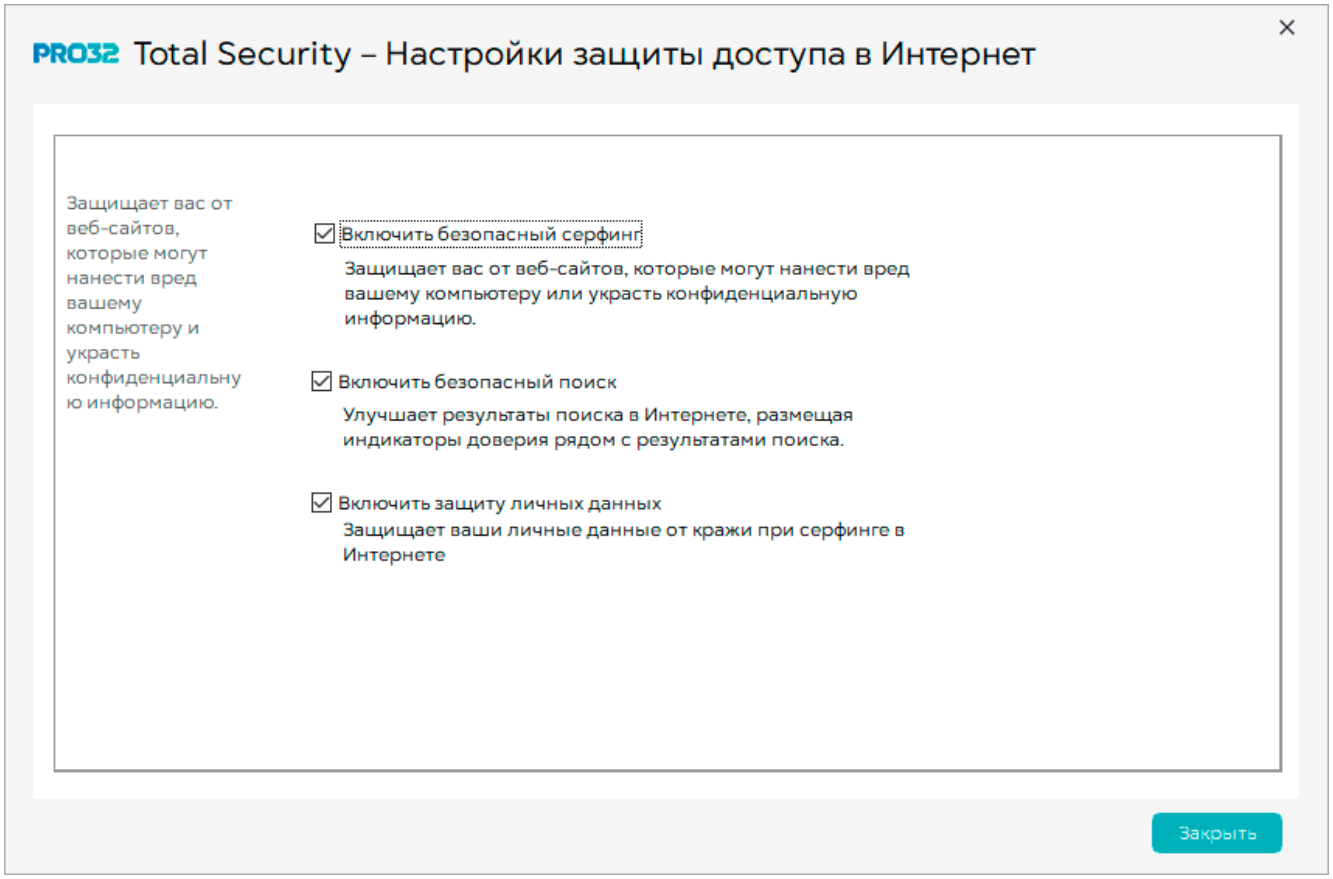
Включение безопасного поиска

Функция безопасного поиска включена по умолчанию. Включенная функция безопасного поиска защищает от веб-сайтов, потенциально содержащих код, который может быть загружен на компьютер или выполнен без вашего согласия. Если по какой-либо причине функция безопасного поиска была отключена, вы всегда можете включить ее повторно.

*Рекомендуется держать функцию безопасного поиска включенной, чтобы обеспечить защиту от веб-сайтов, пытающихся загрузить на компьютер вредоносный контент.

1. Откройте стартовый экран продукта, затем **«Настройки защиты»** > , далее **«Настройки»** > модуля **«Защита доступа в Интернет»**.

2. Откроется диалоговое окно настроек модуля **«Защита доступа в Интернет».**



3. Установите\снимите флажок **«Включить безопасный поиск»** для активации функции.

Настройка блокировки фишинговых сайтов

Безопасный просмотр сайтов активирован по умолчанию. Безопасный просмотр сайтов защищает от веб-сайтов, созданных для того, чтобы вынудить вас обманным путем поделиться личной или финансовой информацией. Если по какой-либо причине функция безопасного просмотра сайтов была отключена, вы всегда можете включить ее повторно.

*Не рекомендуется отключать функцию безопасного поиска, поскольку она обеспечивает защиту от мошеннических веб-сайтов, пытающихся получить от вас конфиденциальную информацию.

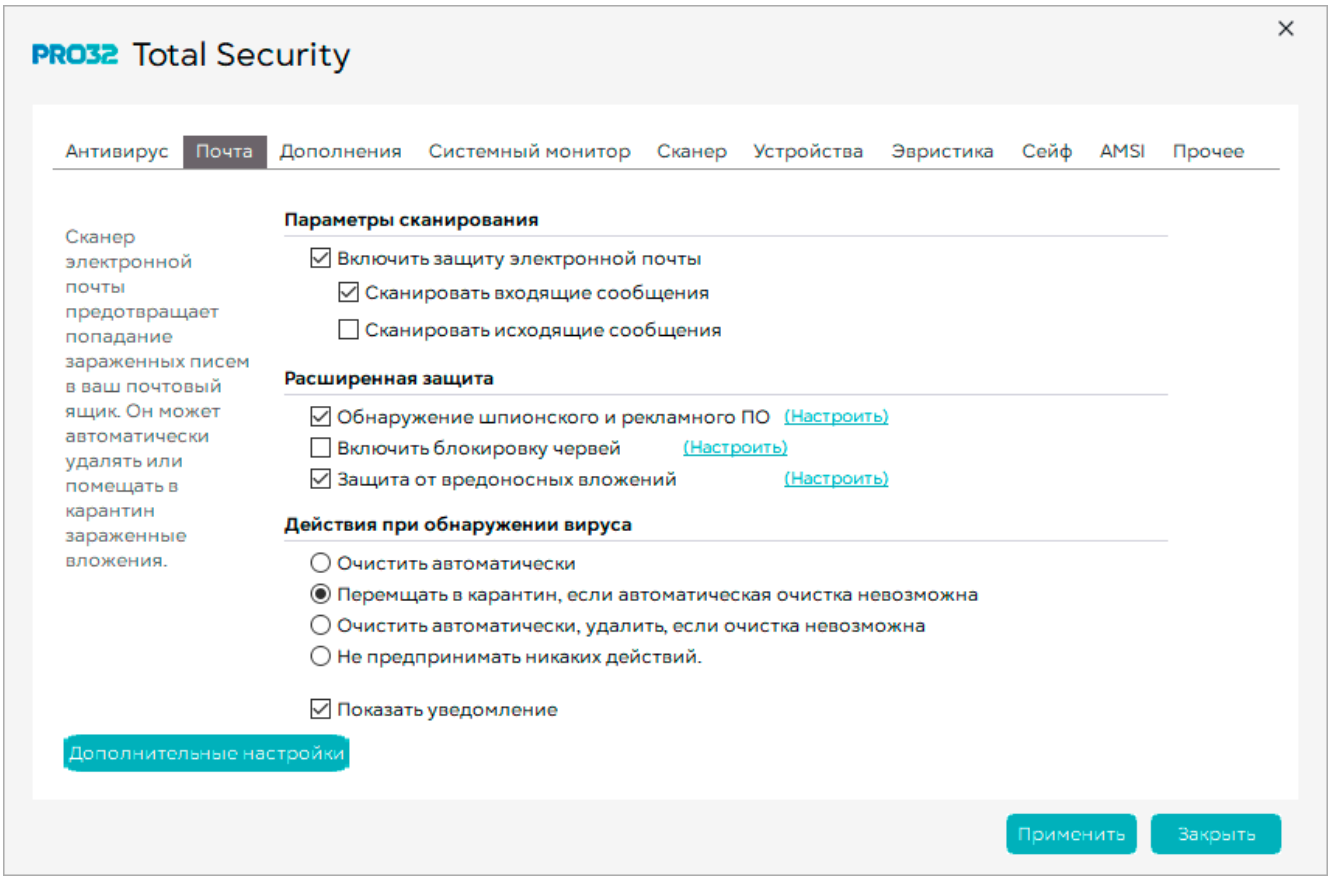
1. Откройте стартовый экран продукта , затем **«Настройки защиты»** , далее **«Настройки»** модуля **«Защита доступа в Интернет»** .

2. Откроется диалоговое окно настроек модуля **«Защита доступа в Интернет».**
3. Установите\снимите флажок **«Включить безопасный серфинг»** для активации функции.

9. Защита электронной почты

Вы можете исключить определенные файлы и области, например, папки или программы, из сканирования:

1. Откройте стартовый экран продукта , затем **«Настройки защиты»** , далее **«Настройки»** модуля **«Антивирус и антишпион»** .
2. Откроется диалоговое окно настроек антивируса.
3. Нажмите вкладку «Почта».



Защита электронной почты включена по умолчанию. Сканер электронной почты проверяет входящие и исходящие электронные письма, чтобы не допустить попадания зараженных писем в ваш почтовый ящик. Если электронное письмо содержит вирус, сканер электронной почты удаляет зараженные вложения или помещает их в карантин.

4. Установите флажок **«Включить защиту электронной почты при запуске Windows»**, чтобы запускать сканер электронной почты при включении компьютера.

5. Установите необходимые флажки, чтобы сканировать входящие и исходящие сообщения электронной почты. Рекомендуется выбрать оба этих параметра, чтобы обеспечить постоянное

отслеживание всех писем электронной почты.

*Примечание: если выбрать сканирование входящих и исходящих сообщений электронной почты без включения защиты электронной почты, сообщения электронной почты сканироваться не будут.

6. В разделе Расширенная защита выберите параметры, которые вы хотите включить в сканирование.

Обнаружение шпионского и рекламного ПО

Сканирует все вложения электронной почты на наличие дополнительных угроз, включая шпионское ПО, рекламное ПО, дозвонщики и т. д. Нажмите «Настроить» рядом с этим параметром, чтобы выбрать тип угроз для сканирования и действия, предпринимаемые при обнаружении таких угроз.

Включить блокировку червей

Предотвращает распространение любых новых вирусов на основе массовой рассылки, проникших в вашу систему, и предупреждает вас об их присутствии. Нажмите «Настроить», чтобы задать способ защиты системы в случае угрозы массовой рассылки.

Защита от вредоносных вложений

Рассматривает вложения в двоичном формате как вредоносные вложения. Нажмите «Настроить» для настройки действия при обнаружении таких вредоносных вложений.

7. В разделе Действие при обнаружении вируса выберите действие, выполняемое системой в случае обнаружения зараженного сообщения электронной почты.

Отображение диалогового окна, если очистка невозможна - Очищает электронную почту без вашего вмешательства. Если выполнить очистку невозможно, вам будет предложено определить предпринимаемое действие.

Перемещать в карантин, если очистка невозможна - Очищает электронную почту без вашего вмешательства. Если выполнить очистку невозможно, файл будет перемещен в папку карантина.

Очистить автоматически, удалить, если очистка невозможна - Очищает электронную почту без вашего вмешательства. Если очистка невозможна, файлы будут удалены.

Не предпринимать никаких действий - Сообщает о заражении, однако никакие действия не предпринимаются. Этот вариант рекомендуется только для опытных пользователей.

Показать уведомление - Установите флажок, чтобы система отображала уведомления при обнаружении вируса.

8. PRO32 Total Security использует встроенный прокси-сервер для обработки сообщений электронной почты. Для настройки параметров сервера нажмите кнопку «Дополнительные Настройки».

9. После настройки сканера электронной почты нажмите «Применить», чтобы сохранить изменения.

9.1 Модуль «Антиспам»

Нежелательная электронная почта, также известная как спам, способна заполнить обычный почтовый ящик с поразительной скоростью. Модуль PRO32AntiSpam идентифицирует и фильтрует нежелательную электронную почту, помечая ее как спам. Он постоянно отслеживает поступающие сообщения электронной почты и отфильтровывает нежелательные. PRO32AntiSpam поддерживает возможность создания черных и белых списков, которые работают в сочетании со спам-фильтром.

Вы можете настроить модуль AntiSpam, указав адреса электронной почты и определенные текстовые строки, которые следует и не следует фильтровать. Например, можно настроить список разрешенных и заблокированных адресов электронной почты, отображаемых имен или доменных имен, которые должны быть разрешены или заблокированы соответственно; настроить фильтры для поиска ключевых слов в заголовках, в теме или теле письма, а также обучить модуль PRO32AntiSpam автоматически определять спам. Когда PRO32AntiSpam обнаруживает сообщение, содержащее один из этих адресов или текстовых строк, сообщение категоризируется в соответствии с вашими настройками. Благодаря этому сообщения от доверенных отправителей не будут помечены как спам.

Состояние функций модуля изображается выключателями . По умолчанию все компоненты и модули продукта включены и имеют преднастроенные правила работы. Для того, чтобы быстро отключить какой-либо модуль, переключите выключатель в состояние «Выкл» .

Выберите время, на которое хотите отключить тот или иной модуль и подтвердите выбор кнопкой **«Да».**

Для настройки модуля:

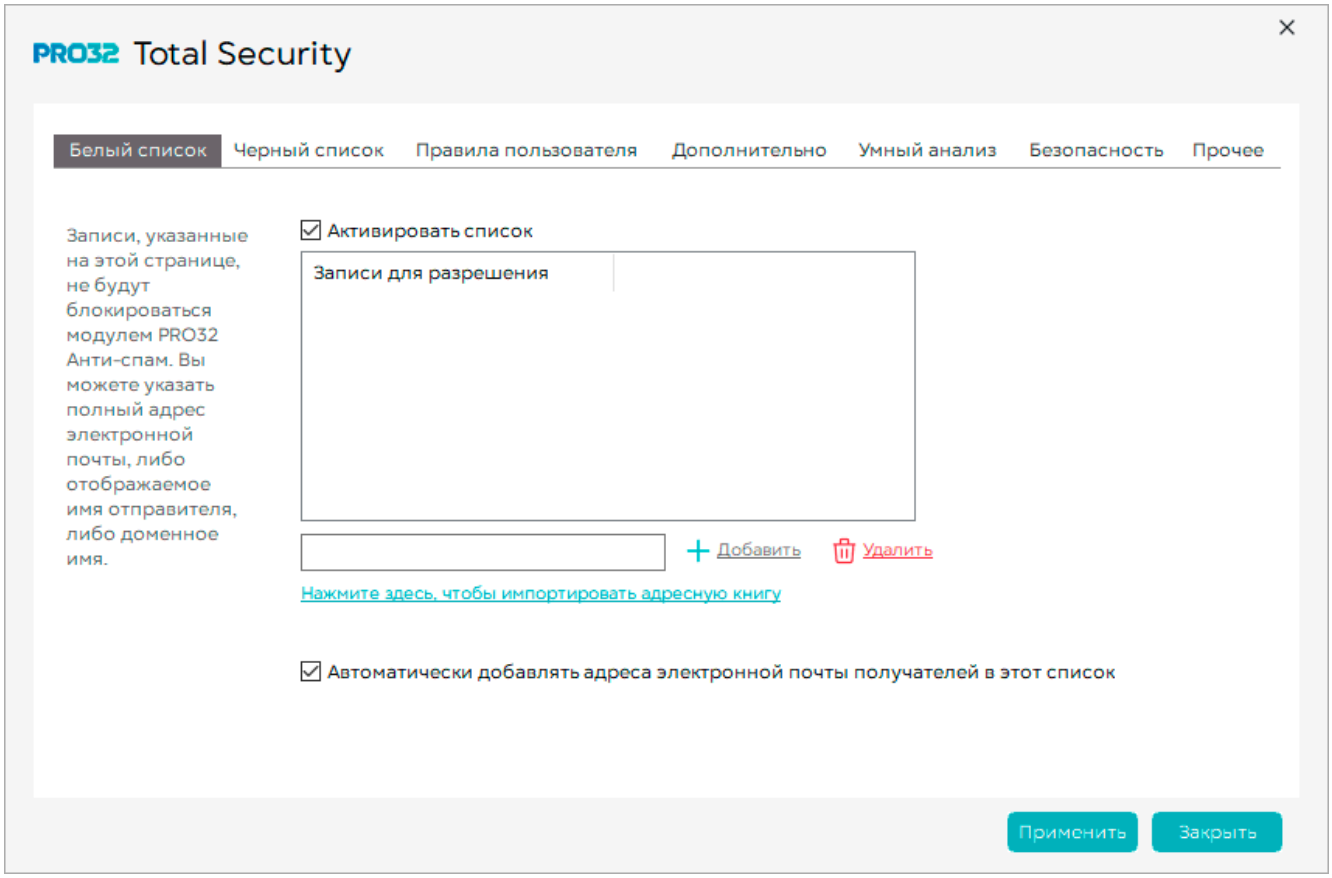
1. Откройте стартовый экран продукта , затем **«Настройки защиты»** , далее **«Настройки»** модуля **«Антиспам»** .

2. Откроется диалоговое окно настроек модуля **«Антиспам».**

3. Можно настроить следующие параметры:

Белый список

Белый список – это список адресов электронной почты или доменных имен, с которых вы хотите получать электронные письма. Вы также можете импортировать адресную книгу из своего почтового клиента в список разрешений.



Чёрный список

Список блокировок – это список адресов электронной почты или доменных имен, с которых вы не хотите получать электронные письма. PRO32AntiSpam помечает все сообщения электронной почты, полученные с этого адреса или домена, как спам.

Правила пользователя

Правила фильтрации спама помогают управлять сообщениями электронной почты, автоматически выполняя действия над сообщениями. PRO32AntiSpam позволяет создавать собственные наборы правил, позволяющие определить, является ли электронное письмо спамом или нет. Правила применяются в том порядке, в котором они отображаются. Вы можете перемещать правила вверх или вниз для изменения последовательности.

Дополнительно

PRO32AntiSpam использует подключение к онлайн-лаборатории для защиты электронной почты от спама и вирусов в режиме реального времени. Это позволяет системе получать информацию о вспышках спама по мере их появления.

Умный анализ

Функция интеллектуального анализа PRO32AntiSpam использует технологию байесовской фильтрации. Она помогает автоматически выявлять спам на основе анализа исходящей электронной почты для определения ваших обычных корреспондентов. Для обработки входящих сообщений электронной почты вам нужно обучить PRO32AntiSpam учитывать личные предпочтения для получения электронной почты. Для этого требуется определенное время.

Безопасность

Фишинговые аферы уже давно известны в Интернете. PRO32AntiSpam можно настроить таким образом, чтобы он блокировал электронные письма, предположительно являющиеся фишинговыми, а также электронные письма, содержащие код и нежелательные вложения.

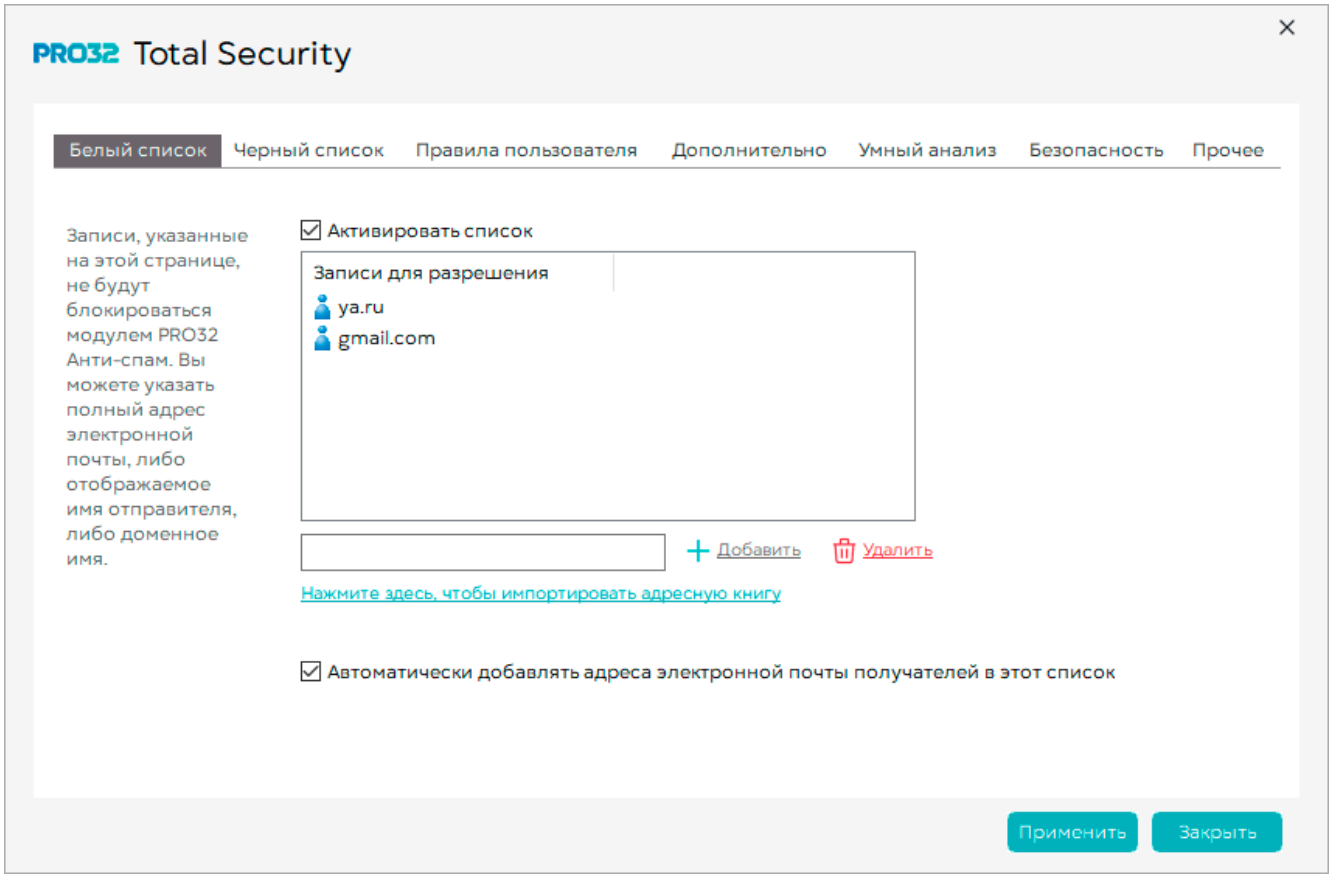
Прочее (интеграция с почтовыми клиентами

PRO32AntiSpam может отслеживать почтовые клиенты POP3 на наличие спама. Поскольку Outlook Express и Microsoft Outlook получили наибольшее распространение, PRO32AntiSpam интегрируется с ними. Во время установки PRO32AntiSpam вставляет панель инструментов для доступа к важным функциям PRO32AntiSpam как в Outlook Express, так и в Microsoft Outlook. Эта панель инструментов PRO32AntiSpam располагается под обычной панелью инструментов.

9.1.1. Белый список

1. Откройте стартовый экран продукта, затем **«Настройки защиты»** > , далее **«Настройки»** > модуля **«Антиспам»** .

2. Откроется диалоговое окно настроек модуля **«Антиспам»** вкладка **«Белый список».**



3. Установите флажок **«Активировать список»,** чтобы активировать список разрешений.

Введите адрес электронной почты, отображаемое имя или доменное имя (например, pro32.com), которые **вы хотите** разрешить, в соответствующем поле и нажмите **«Добавить»** . Запись добавлена в список.

Чтобы удалить запись из белого списка, выберите запись в списке и нажмите кнопку **«Удалить»** . Выбранная запись будет удалена из списка после вашего подтверждения.

Если вы хотите автоматически добавлять адреса электронной почты получателей в список, установите флажок **«Автоматически добавлять адреса электронной почты получателей в этот список».**

Адреса можно импортировать из Outlook Express, Outlook или любого текстового файла с запятыми в качестве разделителей. Нажмите вариант импорт адресной книги. Откроется диалоговое окно Импорт адресной книги. Подробные сведения см. в разделе Импорт адресной книги

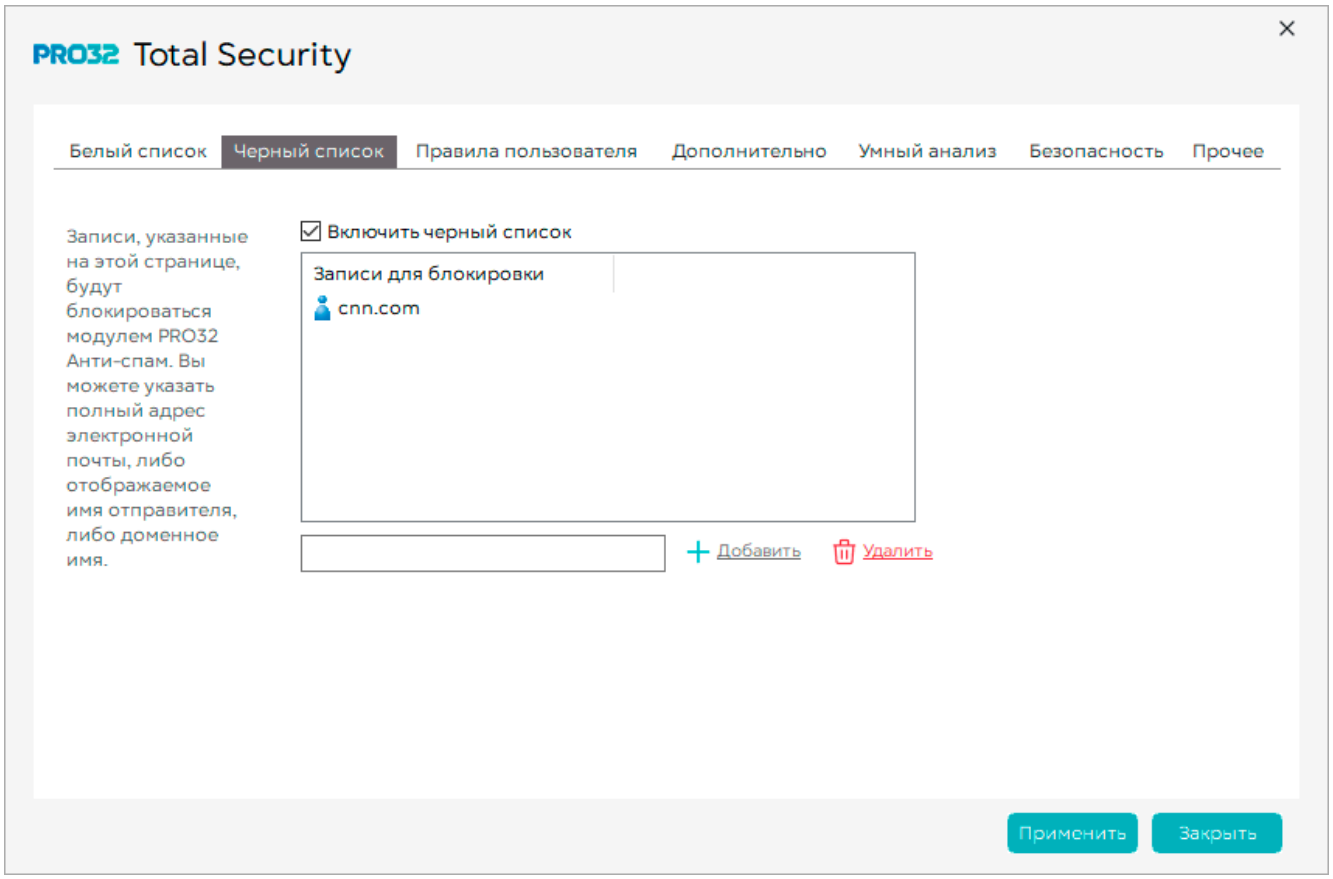
4. Нажмите **«Применить»** для сохранения настроек.

5. Нажмите **«Закрыть»** для закрытия диалогового окна защиты от вредоносного ПО.

9.1.2. Чёрный список

1. Откройте стартовый экран продукта , затем **«Настройки защиты»** , далее **«Настройки»** модуля **«Антиспам»** .

2. Откроется диалоговое окно настроек модуля **«Антиспам»** вкладка **«Чёрный список».**



3. Установите флажок **«Активировать список»,** чтобы активировать список разрешений.

Введите адрес электронной почты, отображаемое имя или доменное имя (например, cheekee-brikee.com), которые **вы НЕ хотите** разрешить, в соответствующем поле и нажмите **«Добавить»** . Запись добавлена в список.

Чтобы удалить запись из белого списка, выберите запись в списке и нажмите кнопку **«Удалить»** . Выбранная запись будет удалена из списка после вашего подтверждения.

4. Нажмите **«Применить»** для сохранения настроек.

5. Нажмите **«Закрыть»** для закрытия диалогового окна защиты от вредоносного ПО.

9.1.3. Пользовательские правила настройки почтового спама

Правила фильтрации спама помогают управлять сообщениями электронной почты, автоматически выполняя действия над сообщениями. PRO32AntiSpam позволяет создавать собственные наборы правил, позволяющие определить, является ли электронное письмо спамом или нет. Правила применяются в том порядке, в котором они отображаются. Вы можете перемещать правила вверх или вниз для изменения последовательности.

Во время установки PRO32AntiSpam интегрируется с MS Outlook или Outlook Express (если вы используете один из этих почтовых клиентов) и создает папку с именем **Сообщения нежелательной почты**. При получении электронного письма PRO32AntiSpam проверяет сообщения и идентифицирует те из них, которые являются спамом. Такие сообщения перемещаются непосредственно в папку «**Сообщения нежелательной почты»**, а не в папку **«Удаленные».**

Когда сообщение определяется как спам, PRO32AntiSpam добавляет текст **[***Spam***]** в начало темы сообщения. Затем вы можете проверить папку **Сообщения нежелательной почты** на наличие сообщений электронной почты, которые были ошибочно идентифицированы как спам, и пометить их как «Не СПАМ». Это позволяет предотвратить удаление сообщений электронной почты из известных источников.

1. Откройте стартовый экран продукта , затем **«Настройки защиты»** , далее **«Настройки»** модуля **«Антиспам»** .

2. Откроется диалоговое окно настроек модуля **«Антиспам»** затем выберите вкладку **«Правила пользователя».**

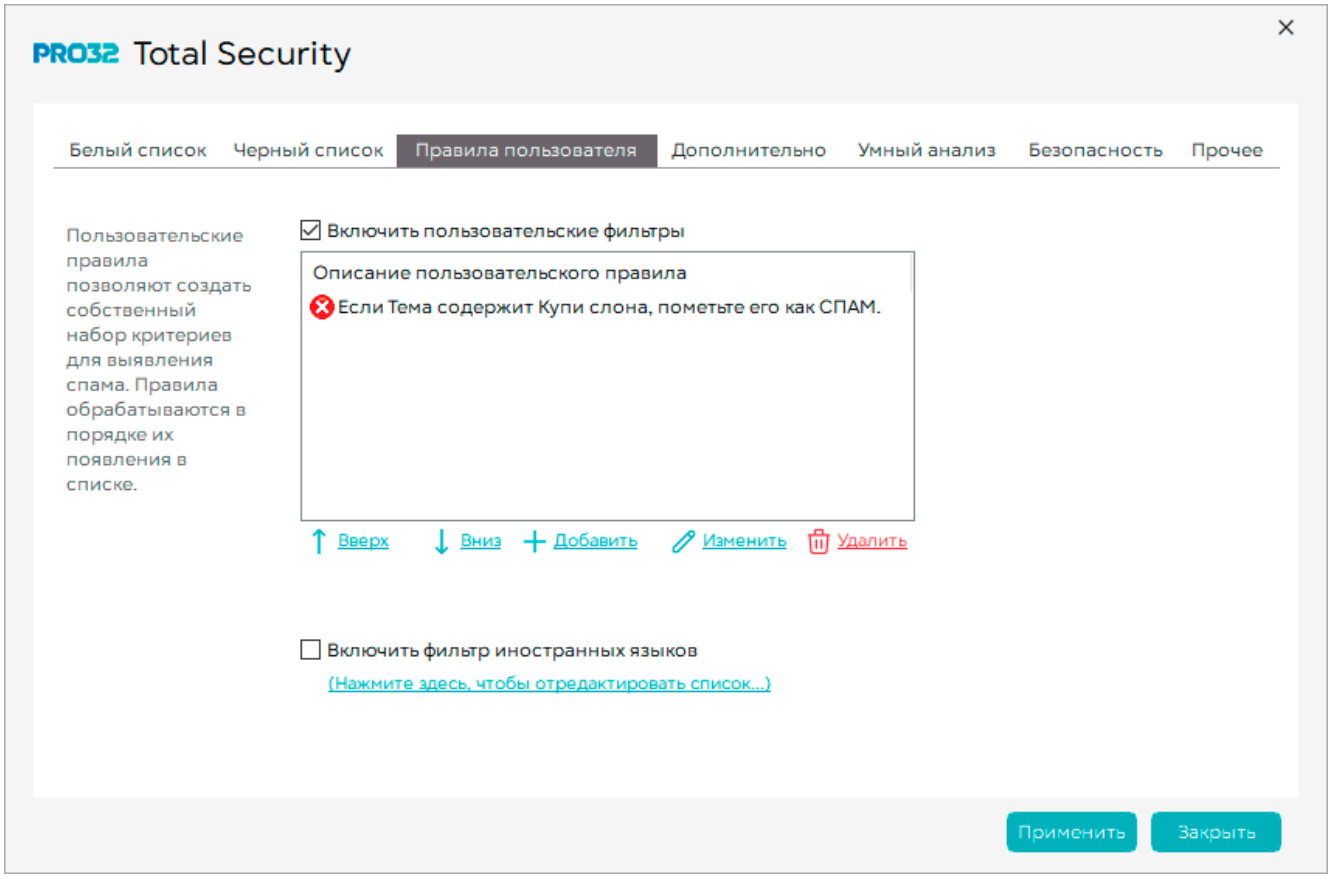
3. Вы можете выбрать одно из следующих действий:

- Создать пользовательские правила фильтрации спама
- Изменить порядок правил фильтрации спама
- Изменить правило фильтрации спама
- Удалить правило фильтрации спама
- Настроить фильтр иностранных языков

4. Установите флажок **«Включить пользовательские фильтры»,** если требуется активировать фильтры. Кнопки на этой странице включены.

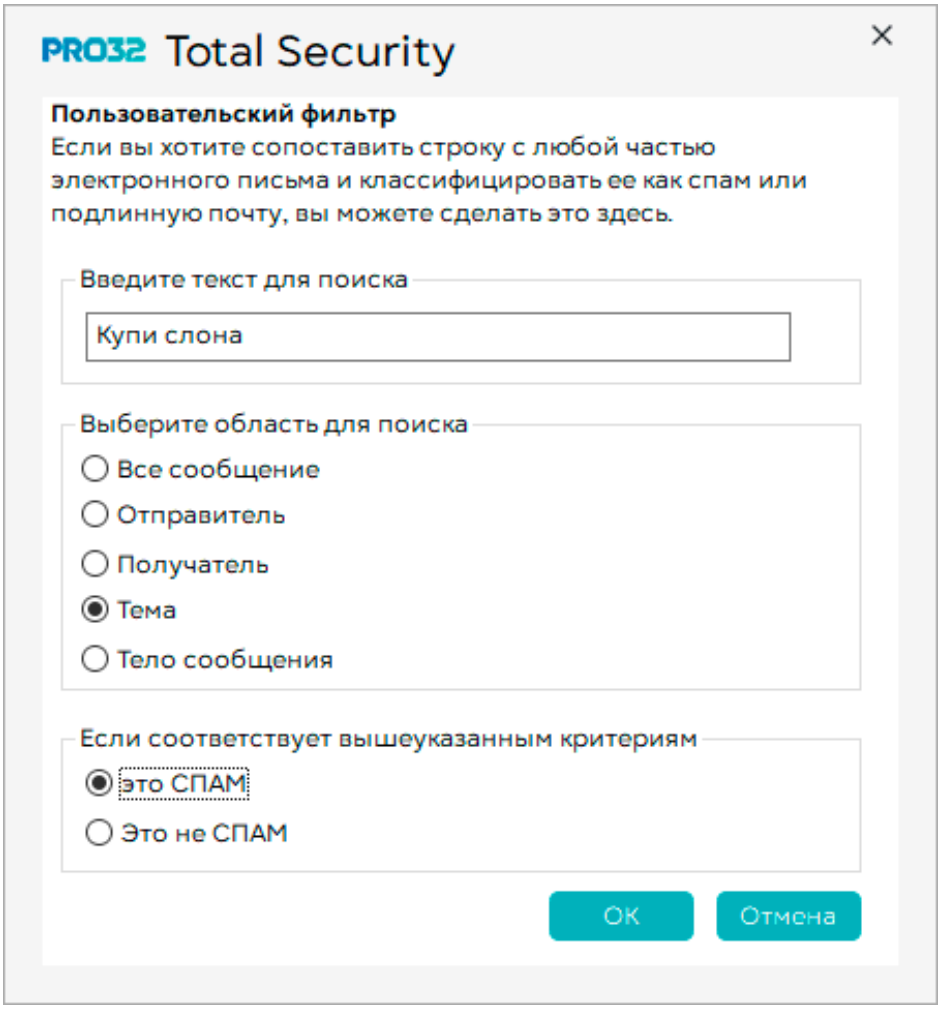
5. Нажмите **«Применить»** для сохранения настроек.

6. Нажмите **«Закрыть»** для закрытия диалогового окна защиты от вредоносного ПО.



Создать пользовательские правила фильтрации спама

1. Нажмите кнопку **«Добавить»** + . Откроется диалоговое окно **«Пользовательский фильтр».**



2. Введите **текст** для поиска.

3. На панели **Область** выберите, где именно во входящих сообщениях электронной почты PRO32AntiSpam нужно искать текст. Параметры описаны в следующей таблице.

Параметр	Описание
По всей почте	Поиск текста во всех сообщениях электронной почты
Адрес отправителя	Поиск текста в адресах отправителей
Адрес получателя	Поиск текста в адресах получателей
Строка темы	Поиск текста в строках темы сообщений
Тело сообщения	Поиск текста только в теле сообщения электронной почты

4. Выберите, как вы хотите классифицировать электронные письма, которые соответствуют критериям, определенным выше. Доступные варианты:

Является спамом– классифицирует электронное письмо как **спам** при совпадении критериев

Не является спамом– классифицирует электронное письмо как **не спам** при совпадении критериев

5. Нажмите **«ОК»**, чтобы сохранить правило и вернуться к диалоговому окну «**Настройка защиты от спама».** Правило добавляется и описывается в разделе **Описание пользовательского правила**.

Изменить порядок правил фильтрации спама

PRO32AntiSpam сравнивает входящее сообщение электронной почты со списком правил для спама. Правила применяются в том порядке, в котором они отображаются в списке правил. Сначала применяется правило, расположенное в верхней части списка, затем происходит движение вниз по списку, пока не будет найдено соответствие.

После того, как соответствие будет найдено, PRO32AntiSpam классифицирует сообщение электронной почты соответствующим образом и переходит к следующему сообщению. Вы можете обнаружить, что получаемые вами нежелательные сообщения соответствуют одному из правил чаще, чем другим. В таком случае вы можете переместить это правило в начало списка.

1.Откройте стартовый экран продукта , затем **«Настройки защиты»** , далее **«Настройки»** модуля **«Антиспам»** .

2. Откроется диалоговое окно настроек модуля **«Антиспам»** затем выберите вкладку **«Правила пользователя».**

3. Выберите правило, порядок которого вы хотите изменить, и нажмите кнопку Вверх или Вниз , чтобы переместить правило на одну ступень вверх или вниз, пока оно не окажется в нужном вам положении.

Изменить правило фильтрации спама

1.Откройте стартовый экран продукта , затем **«Настройки защиты»** , далее **«Настройки»** модуля **«Антиспам»** .

2. Откроется диалоговое окно настроек модуля **«Антиспам»** затем выберите вкладку **«Правила пользователя».**

3. Выберите правило и нажмите кнопку **«Редактировать»** . Откроется диалоговое окно **«Пользовательский фильтр».**

4. Внесите необходимые изменения.

5. Нажмите **«ОК»**, чтобы сохранить правило и вернуться к диалоговому окну «**Настройка защиты от спама».** Правило добавляется и описывается в разделе **Описание пользовательского правила**.

Удалить правило фильтрации спама

1.Откройте стартовый экран продукта , затем **«Настройки защиты»** , далее **«Настройки»** модуля **«Антиспам»** .

2. Откроется диалоговое окно настроек модуля **«Антиспам»** затем выберите вкладку **«Правила пользователя».**

3. Выберите правило и нажмите кнопку **«Удалить»** . После вашего подтверждения правило будет удалено.

Настроить фильтр иностранных языков

Если вы получаете нежелательные письма на иностранных языках, вы можете создать фильтр для проверки языка писем. Вы можете заблокировать все электронные письма, составленные на определенном языке (языках).

1.Откройте стартовый экран продукта , затем **«Настройки защиты»**, далее **«Настройки»** модуля **«Антиспам»** .

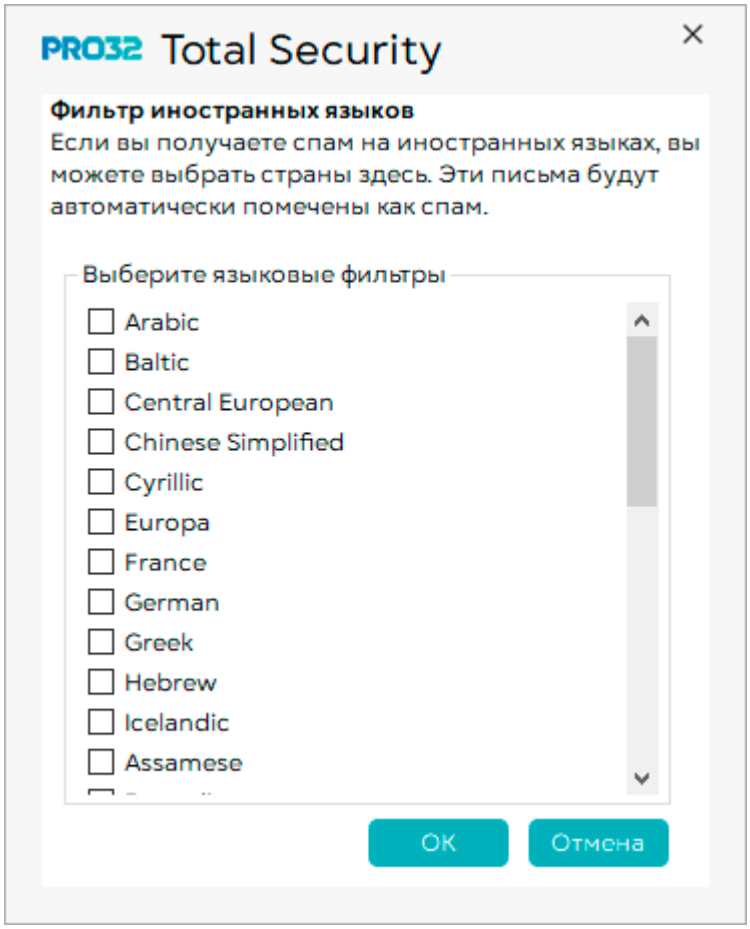
2. Откроется диалоговое окно настроек модуля **«Антиспам»** затем выберите вкладку **«Правила пользователя».**

4. Установите флажок **«Включить фильтр иностранных языков».** Язык каждого письма будет сравниваться с настроенным.

5. Нажмите параметр **«Изменить»** под флажком для добавления или удаления языков. Откроется диалоговое окно **«Фильтр иностранных языков».**

6. Установите соответствующие флажки, чтобы включить в фильтр требуемые языки. Если вы хотите получать почту на определенном языке, снимите флажок для этого языка.

7. Нажмите **«ОК»** для сохранения фильтра.



9.1.4. Настройка анализа нежелательной почты в режиме онлайн

PRO32AntiSpam использует подключение к онлайн-лаборатории для защиты электронной почты от спама и вирусов в режиме реального времени. Это позволяет системе получать информацию о вспышках спама по мере их появления.

PRO32AntiSpam отправляет в онлайн-лабораторию определенные сведения о каждом электронном письме (но не его содержание). Сообщение электронной почты сравнивается с сообщениями, полученными со всего мира. При наличии нескольких похожих писем они помечаются как спам.

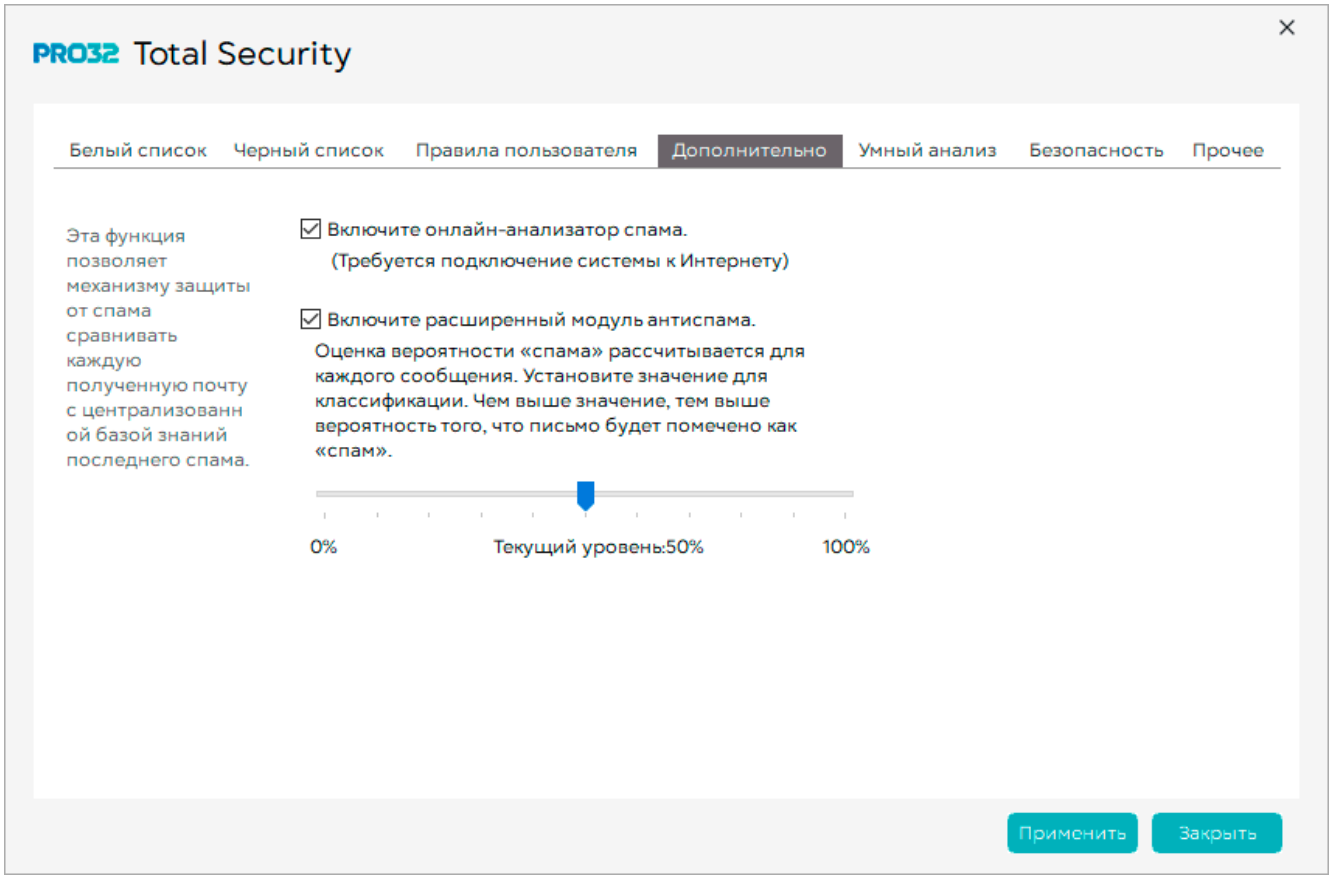
1. Откройте стартовый экран продукта, затем **«Настройки защиты»** > , далее **«Настройки»** > модуля **«Антиспам»**.

2. Откроется диалоговое окно настроек модуля **«Антиспам»** затем выберите вкладку **«Дополнительно».**

3. Установите флажок **«Включить онлайн- анализатор спама».**

*Примечание: для подключения к онлайн-анализатору спама требуется доступ к Интернету.

4. Нажмите кнопку **«Применить».**



9.1.5. Настройка интеллектуального анализа

Функция интеллектуального анализа PRO32AntiSpam использует технологию байесовской фильтрации. Она помогает автоматически выявлять спам на основе анализа исходящей электронной почты для определения ваших обычных корреспондентов. Для обработки входящих сообщений электронной почты вам нужно обучить PRO32AntiSpam учитывать личные предпочтения для получения электронной почты. Для этого требуется определенное время.

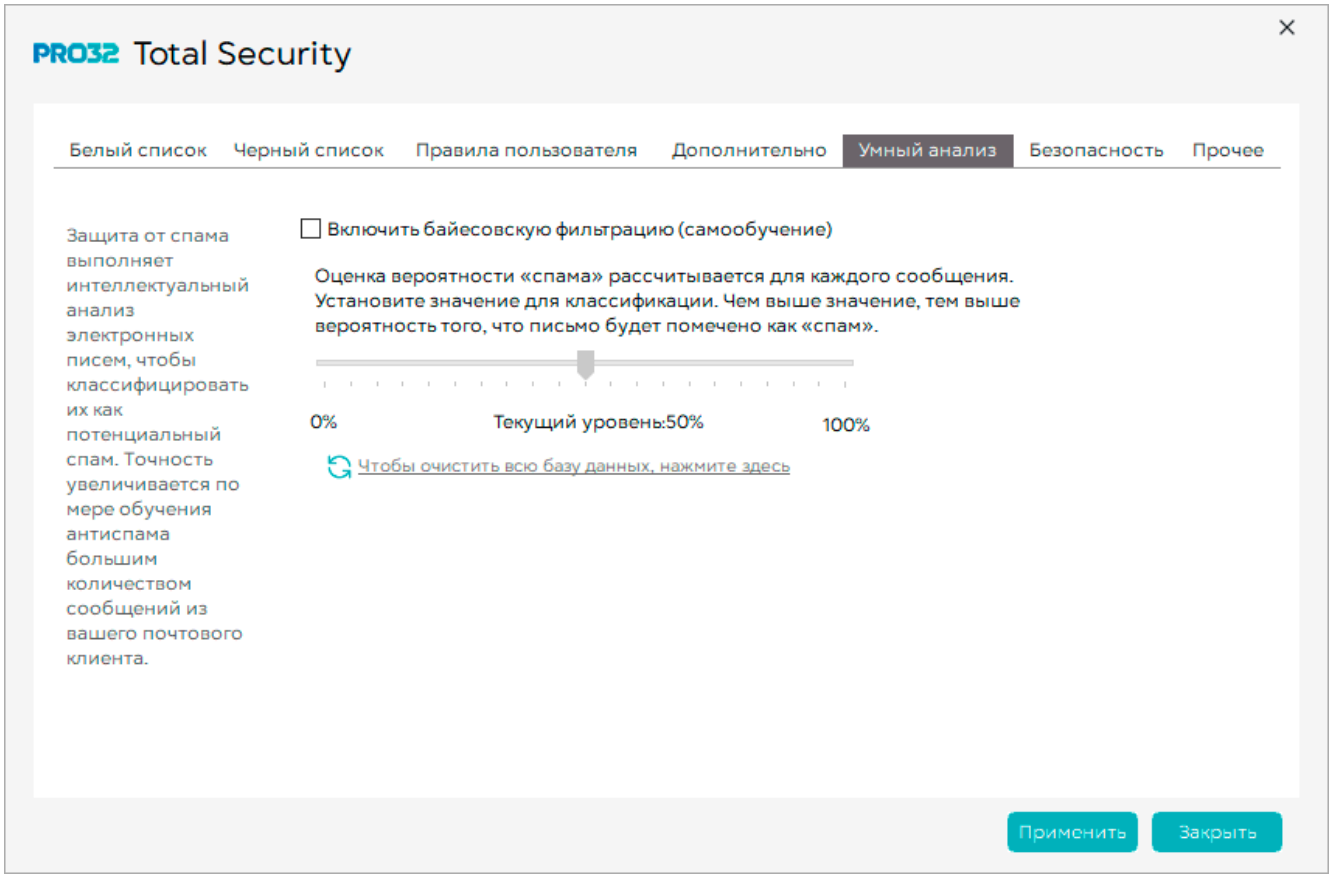
PRO32Antispam использует байесовскую технологию для сравнения содержимого входящих сообщений электронной почты, чтобы помечать их как спам. Сообщения оцениваются на основе того, какие из их характеристик больше похожи на спам. Когда количество характеристик «Спам» больше, чем характеристик «Не спам», сообщение будет помечено как нежелательное. Вы можете указать коэффициент, используемый для выявления спама. Когда этот коэффициент низкий, электронные письма помечаются как спам, то есть обнаруживается меньше характеристик спама.

1.Откройте стартовый экран продукта , затем **«Настройки защиты»**, далее **«Настройки»** модуля **«Антиспам»** .

2. Откроется диалоговое окно настроек модуля **«Антиспам»** затем выберите вкладку **«Умный анализ».**

3. Установите флажок **«Включить байесовские фильтры».**

С помощью ползунка установите соотношение, которое будет использоваться при проверке характеристик спама. Чем выше коэффициент, тем больше вероятность того, что сообщение является спамом.



4. Также Вы можете: Сбросить базу знаний

5. Нажмите **«Применить»** для сохранения настроек.

6. Нажмите **«Закрыть»** для закрытия диалогового окна защиты от спама.

Обучение модуля интеллектуального анализа

Для обработки входящих сообщений электронной почты вы можете обучить PRO32AntiSpam учитывать личные предпочтения для получения электронной почты. Для этого требуется определенное время. Технология байесовского фильтра, используемая модулем PRO32AntiSpam, создает базу знаний для определения характеристик спама. Вы можете обучать базу знаний, помечая как можно больше законных писем как «Не спам», а нежелательных писем – как «Спам». Для этого используйте панель инструментов PRO32AntiSpam, создаваемую под обычной панелью инструментов в Outlook Express и Outlook.

Для обучения модуля интеллектуального анализа

1. Откройте свой почтовый клиент – Outlook или Outlook Express.

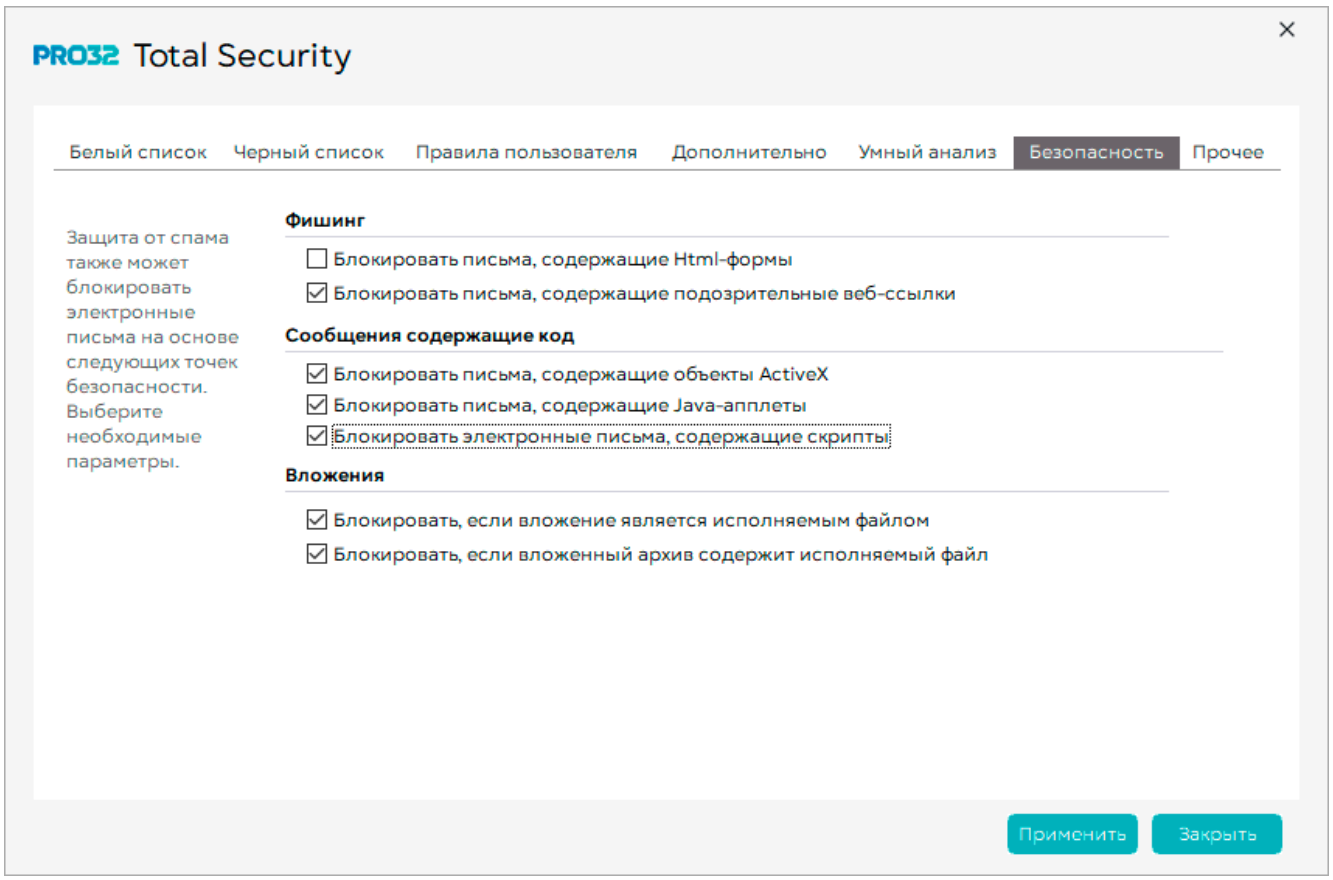
2. Выберите письмо, которое хотите пометить как спам, и нажмите кнопку **«Это спам»** на панели инструментов PRO32AntiSpam.

9.1.5. Безопасность

Фишинговые аферы уже давно известны в Интернете. PRO32AntiSpam можно настроить таким образом, чтобы он блокировал электронные письма, предположительно являющиеся фишинговыми, а также электронные письма, содержащие код и нежелательные вложения.

1.Откройте стартовый экран продукта , затем **«Настройки защиты»**, далее **«Настройки»** модуля **«Антиспам»** .

2. Откроется диалоговое окно настроек модуля **«Антиспам»** затем выберите вкладку **«Безопасность».**



3. Параметры безопасности подробно описаны в следующей таблице:

Безопасность	Параметр	Описание
Фишинг	**Блокировать сообщения электронной почты, содержащие HTML-формы**	Блокирует сообщения электронной почты, содержащие HTML-формы. Для сбора данных используются HTML-формы.
	Блокировать сообщения электронной почты, содержащие подозрительные веб-ссылки	Блокирует сообщения электронной почты со ссылками на нежелательные сайты.
Сообщения электронной почты со встроенным кодом	**Блокировать электронные письма, содержащие объекты ActiveX**	Блокирует сообщения электронной почты, содержащие элементы управления ActiveX – они могут загружать нежелательные программы.
	Блокировать электронные письма, содержащие Java-апплеты	Блокирует сообщения электронной почты с Java-апплетами – они могут похищать личную информацию с ПК.

	Блокировать электронные письма, содержащие скрипты	Блокирует сообщения электронной почты, содержащие скрипты – они могут записывать файлы cookie и отслеживать личные привычки просмотра.
Вложения	**Блокировать, если вложение является программным файлом**	Блокирует сообщения электронной почты с программными файлами в виде вложений – подлинные программы обычно не передаются по электронной почте, скорее всего, это вирус
	Блокировать, если архивное вложение является программным файлом	Блокирует электронные письма с вложениями Zip, содержащими программы – при открытии Zip-файла программы могут запускаться.

4. Нажмите **«Применить»** для сохранения настроек.

5. Нажмите **«Закрыть»** для закрытия диалогового окна защиты от вредоносного ПО.

9.1.6. Интеграция с почтовым клиентом

PRO32AntiSpam может отслеживать почтовые клиенты POP3 на наличие спама. Поскольку Outlook Express и Microsoft Outlook получили наибольшее распространение, PRO32AntiSpam интегрируется с ними. Во время установки PRO32AntiSpam вставляет панель инструментов для доступа к важным функциям PRO32AntiSpam как в Outlook Express, так и в Microsoft Outlook. Эта панель инструментов PRO32AntiSpam располагается под обычной панелью инструментов

1. Откройте стартовый экран продукта , затем **«Настройки защиты»**, далее **«Настройки»** модуля **«Антиспам»** .

2. Откроется диалоговое окно настроек модуля **«Антиспам»** затем выберите вкладку **«Прочее».**

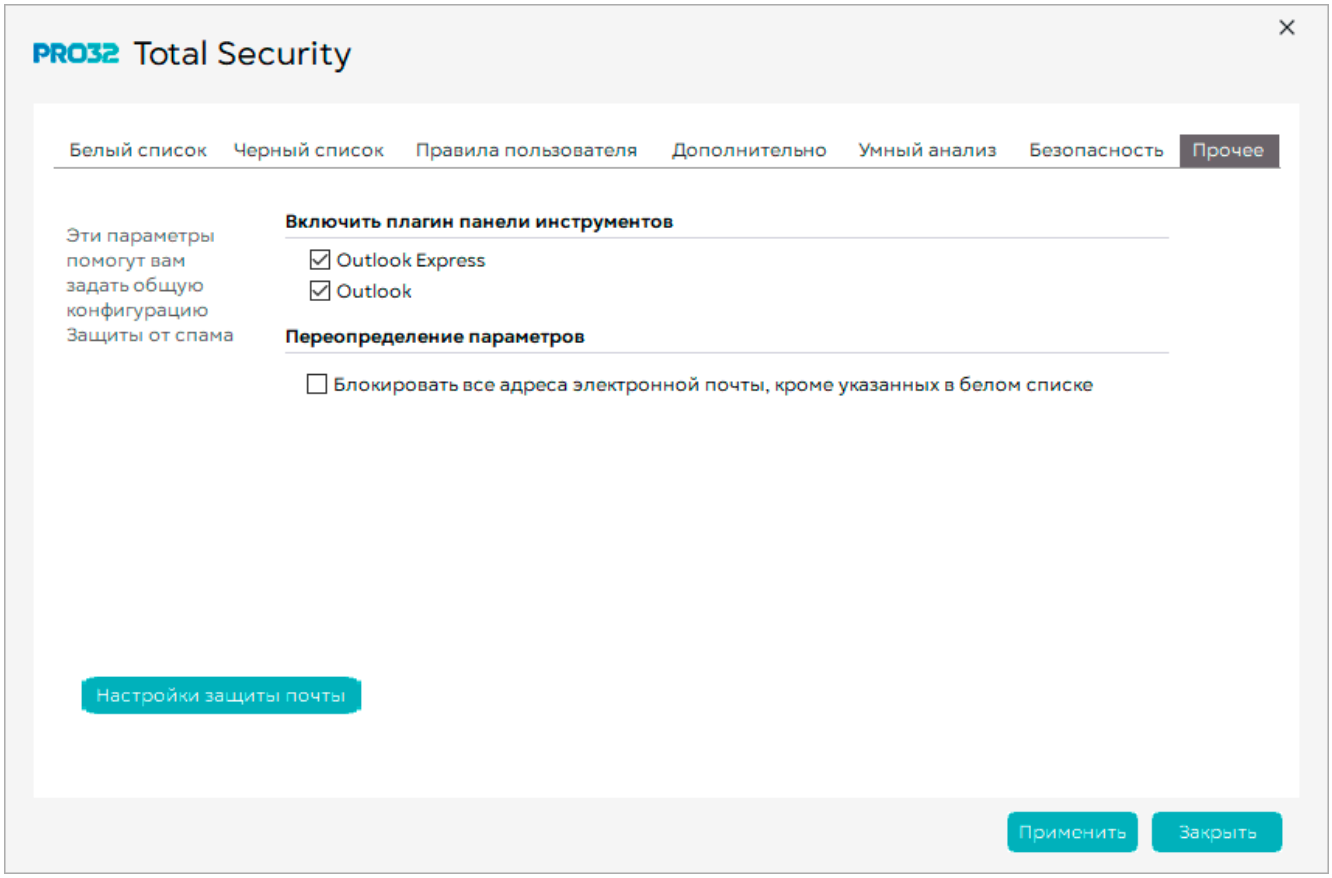
3. Установите флажки для следующих параметров в разделе **«Включить плагин панели инструментов»**:

- **Outlook Express** – создает панель инструментов PRO32AntiSpam в Outlook Express.
- **Outlook** –создает панель инструментов PRO32AntiSpam в Microsoft Outlook

По умолчанию флажки установлены. Для удаления панели инструментов из почтового клиента снимите соответствующий флажок.

5. Нажмите **«Применить»** для сохранения настроек.

6. Нажмите **«Закрыть»** для закрытия диалогового окна защиты от вредоносного ПО.



7. Откройте почтовый клиент. Под обычной панелью инструментов будет отображаться панель PRO32AntiSpam.

8. Вы можете помечать письма как **«Это спам»** или **«Это не спам»** в своем почтовом клиенте.

9. Чтобы все электронные письма, соответствующие адресу в списке разрешенных, попадали в папку Входящие, и чтобы блокировать все остальные электронные письма, установите флажок **«Блокировать все электронные письма, кроме тех, которые присутствуют в белом списке».** Выбор этого параметра переопределит все другие конфигурации.

6. Защита от спама использует встроенный прокси-сервер для обработки электронной почты. Электронные письма сканируются на вирусы и фильтруются анти-спам модулем, а затем отправляются в ваш почтовый клиент. Для настройки параметров сервера электронной почты нажмите кнопку **«Настройки электронной почты».**

10. Модуль «Защита веб-камеры»

Защита веб-камеры от PRO32 позволяет пользователю блокировать любое несанкционированное использование веб-камеры хакерами или ненадежными приложениями для предотвращения шпионажа.

Откройте стартовый экран продукта , затем **«Настройки защиты»**, далее найдите модуль **«Защита веб-камеры»** . Состояние функций модуля изображается выключателями . По умолчанию все компоненты и модули продукта включены и имеют преднастроенные правила работы. Для того, чтобы быстро отключить какой-либо модуль, переключите выключатель в состояние «Выкл» .

Выберите время, на которое хотите отключить тот или иной модуль и подтвердите выбор кнопкой **«Да».**

Для настройки модуля:

1.Откройте стартовый экран продукта , затем **«Настройки защиты»**, далее **«Настройки»** модуля **«Защита веб-камеры»** .

2. Откроется диалоговое окно настроек модуля **«Защита веб-камеры».**

3. По умолчанию флажок «Включить защиту веб-камеры» активен. Вы можете отключить модуль сняв его.

4. Вы можете заблокировать все приложения, использующие камеру выбрав режим **«Заблокировать всё»**

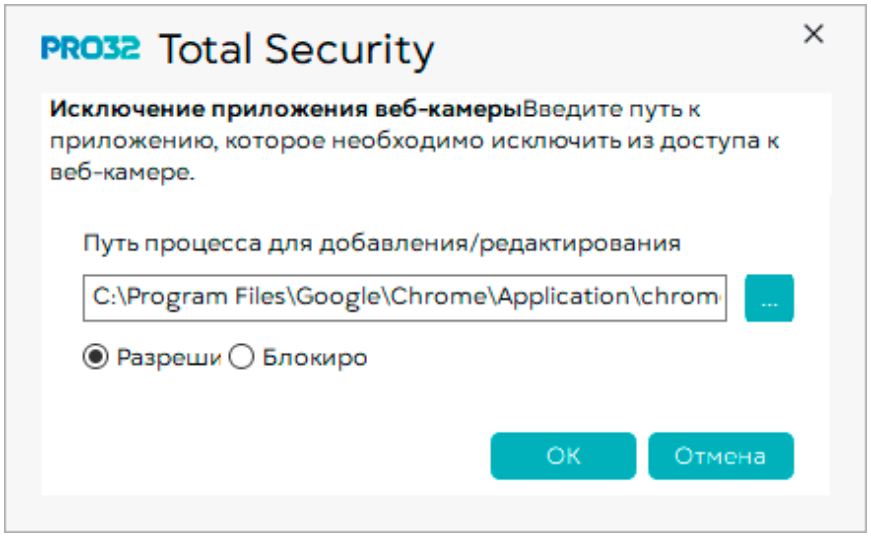
5. Вы можете заблокировать\разблокировать приложения, использующие камеру по выбору, используя «**Ограниченный режим».**

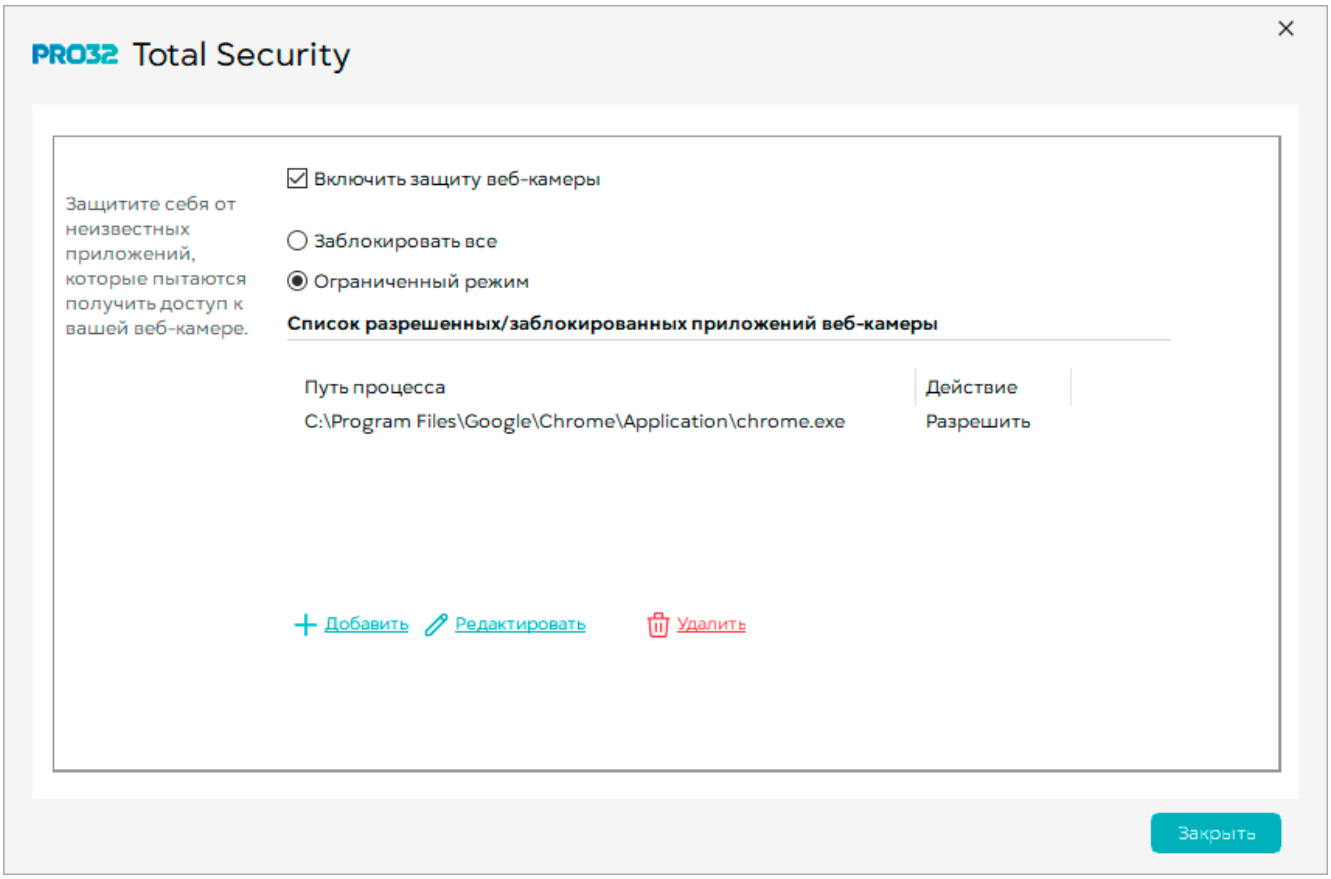
Нажмите кнопку **«Добавить»** . Откроется диалоговое окно «**Исключение приложения веб-камеры»** Введите путь к приложению, которое необходимо исключить из доступа к веб-камере нажав кнопку ....

Укажите путь к исполняемому файлу приложения, использующего камеру, затем выберите **«Разрешить»** или **«Блокировать».**

Для применения правила нажмите кнопку **«ОК».**

2. Вы можете изменять правило нажав кнопку **«Редактировать»** .





11. Модуль «Родительский контроль»

Функция родительского контроля позволяет блокировать веб-сайты и приложения/игры, а также защищать детей от доступа к нежелательной информации. Эта функция позволяет фильтровать веб-сайты, использующие протокол http и https. Вы также можете блокировать доступ сторонних браузеров к Интернету.

Откройте стартовый экран продукта, затем **«Настройки защиты»**, далее найдите модуль **«Родительский контроль»**. Состояние функций модуля изображается выключателями.

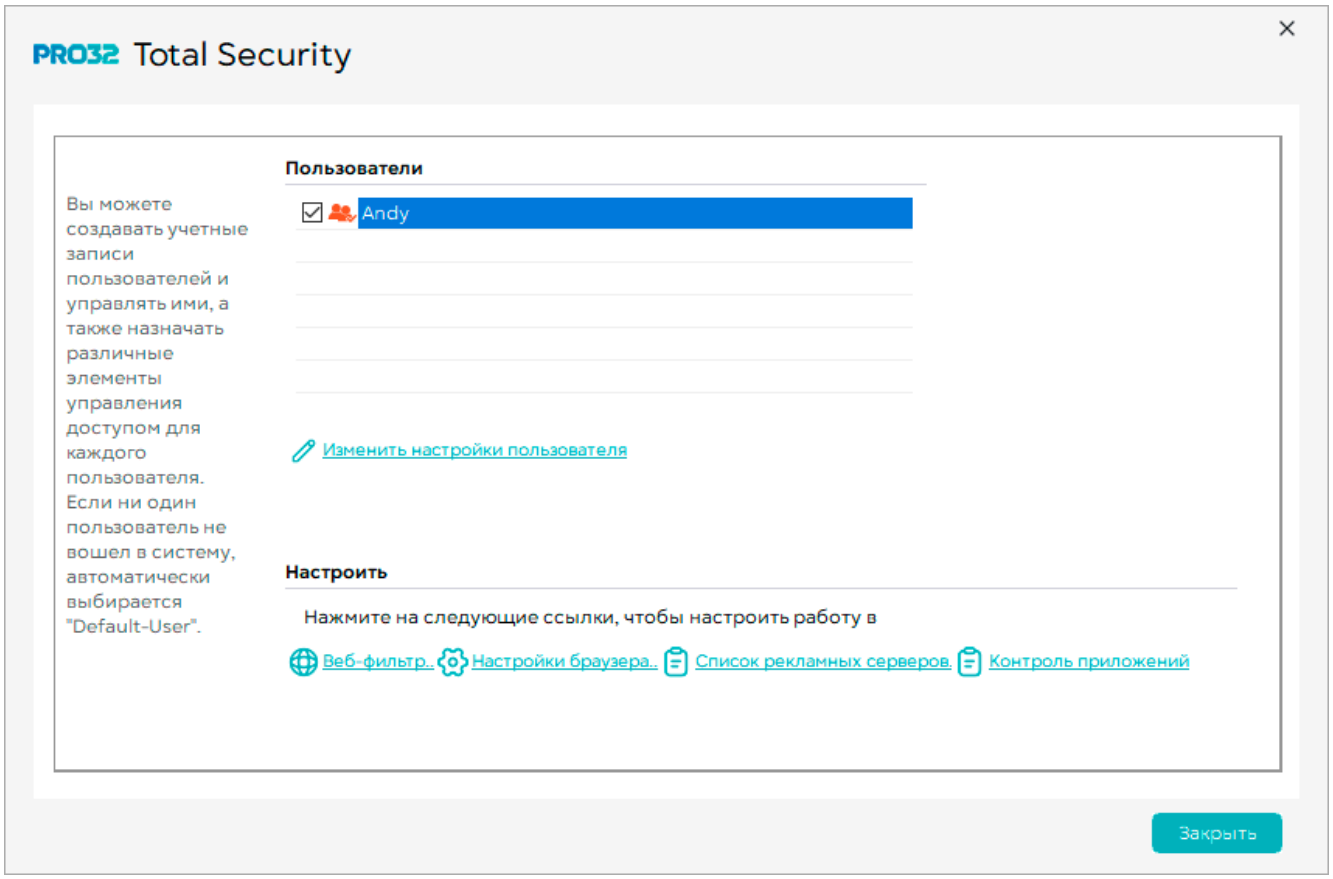
По умолчанию все компоненты и модули продукта включены и имеют преднастроенные правила работы. Для того, чтобы быстро отключить какой-либо модуль, переключите выключатель в состояние «Выкл».

Выберите время, на которое хотите отключить тот или иной модуль и подтвердите выбор кнопкой **«Да».**

Функция родительского контроля позволяет блокировать веб-сайты и приложения/игры, а также защищать детей от доступа к нежелательной информации. Если вы отключите функцию родительского контроля по какой-либо причине, вы можете включить ее снова.

Примечание: рекомендуется включить функцию родительского контроля, чтобы предотвратить попадание личной информации в Интернет.

2. Откроется диалоговое окно настроек модуля **«Родительский контроль».**



Вам доступны следующие действия:

- Редактирование профилей пользователей
- Настройка веб-фильтра
- Настройка параметров браузера
- Настройка списка серверов объявлений
- Настройка параметров конфиденциальности для пользователя
- Настройка управления приложением для пользователя

11.1. Настройка профилей пользователей

Если компьютер находится в совместном использовании несколькими людьми, вы можете создать учетные записи, соответствующие потребностям каждого пользователя, и настроить их

соответствующим образом. Вы можете создавать индивидуальные настройки для отдельных членов семьи.

При установке модуля PRO32Privacy программа создает учетную запись с правами администратора. Существует также учетная запись по умолчанию, а именно Default-User. Когда любой пользователь выходит из системы, активируются настройки для пользователя по умолчанию, которые будут действовать до тех пор, пока в систему не войдет другой пользователь. Вы можете изменить настройки для этой учетной записи по умолчанию.

Если компьютером пользуются несколько людей, вы можете создать отдельные учетные записи для каждого пользователя или же создать группу пользователей с одинаковыми правами и выполнить соответствующую настройку доступа.

Для настройки модуля:

1. Откройте стартовый экран продукта , затем **«Настройки защиты»**, далее найдите модуль **«Родительский контроль»** . Затем нажмите на кнопку **«Настройки»** модуля **«Родительский контроль».**

2. Откроется диалоговое окно настроек модуля **«Родительский контроль»** затем выберите вкладку **«Изменить настройки пользователя»** .

4. Вы можете настроить способ обработки конфиденциальной информации для учетной записи, параметры браузера, веб-фильтр, контроль приложений и время нахождения в Интернете для выбранного пользователя.

5. Чтобы указать действие, выполняемое при обнаружении отправки конфиденциальной информации после входа пользователя в систему, выберите параметр на вкладке Конфиденциальность. Параметры описаны в следующей таблице:

Параметр	Описание
Разрешить отправку конфиденциальной информации только на доверенные веб-сайты	Разрешает отправку конфиденциальной информации, относящейся к пользователю, на доверенные веб-сайты, указанные в разделе «Защита идентификационной информации».
При отправке на другие веб-сайты запрашивать действие	Запрашивает действие при отправке конфиденциальной информации на веб-сайты, отличные от указанных в разделе «Защита идентификационной информации».
При отправке на другие сайты блокировать информацию	Блокирует отправку конфиденциальной информации, относящейся к пользователю, на любые веб-сайты, отличные от указанных в разделе «Защита идентификационной информации».
Блокировать отправку любой конфиденциальной информации	Блокирует отправку любой конфиденциальной информации на любые веб-сайты.
Уведомлять при блокировке указанной выше информации	Установите этот флажок, если вы хотите получать уведомления о блокировке отправки конфиденциальной информации.

Отключить защиту конфиденциальной информации	(Не рекомендуется) Выберите этот вариант, чтобы не ограничивать отправку конфиденциальной информации на любые веб-сайты.

6. Чтобы указать параметры для пользователя при доступе к веб-сайтам, нажмите вкладку Настройки браузера и выберите требуемые параметры. Свойства браузера описаны в следующей таблице.

Свойство	Параметр	Описание
Действия с файлами cookie	**Разрешить все файлы cookie**	Разрешает файлы cookie
	Блокировать все файлы cookie	Блокирует файлы cookie
Действия с элементами управления Active-X	**Разрешить все элементы ActiveX**	Разрешает элементы управления Active-X
	Заблокировать все элементы ActiveX	Блокирует элементы управления Active-X
	Запрашивать действие	Всегда запрашивает действие с элементами управления ActiveX
Действия с Java-апплетами	**Разрешить все Java-апплеты**	Разрешает Java-апплеты
	Блокировать все Java-апплеты	Блокирует Java-апплеты
	Запрос действия	Всегда запрашивает действие с Java-апплетами
Блокировка рекламы	**Блокирует рекламные объявления**	Установите флажок, чтобы не отображать рекламу при доступе к веб-сайтам.

7. Чтобы настроить параметры веб-фильтра для пользователя, выберите вкладку Веб-фильтр. Параметры описаны ниже.

Параметр	Описание
Не фильтровать сайты	Позволяет просматривать все сайты без ограничений
Разрешить сайты из списка разрешений	Разрешает просмотр всех сайтов, перечисленных в списке разрешений, при этом все остальные сайты будут заблокированы для этого пользователя
Блокировать сайты из списка блокировок	Блокирует сайты, перечисленные в списке блокировок, и разрешает доступ ко всем остальным сайтам
Регистрировать все посещенные веб-сайты	Записывает в журнал все веб-сайты, посещенные этим пользователем

8. Если вы хотите задать время, когда пользователю разрешено выходить в Интернет, перейдите на вкладку Время.

9. Если вы хотите указать приложения/браузеры, доступные пользователю, нажмите на вкладку Контроль приложений.

Параметр	Описание
Не фильтровать приложения	Пользователь может получать доступ к любым приложениям/выполнять любые приложения
Разрешить только приложения из списка разрешений	Разрешает пользователю доступ только к тем приложениям, которые указаны в списке разрешенных приложений.
Блокировать только приложения из списка блокировок	Запрещает пользователю доступ только к тем приложениям, которые указаны в списке заблокированных приложений.
Регистрировать все заблокированные приложения	Записывает в журнал все попытки доступа пользователя к приложениям из списка заблокированных приложений.
Управление веб-браузером	Выберите этот параметр для фильтрации веб-сайтов https, добавленных в список разрешенных или заблокированных. Другим веб-браузерам, кроме Internet Explorer, не будет разрешен доступ в Интернет.

11.2. Настройка веб-фильтра

Доступ к различным веб-сайтам можно ограничить. Существует два способа ограничить доступ к веб-сайтам:

• Список разрешений: этот список содержит сайты, к которым пользователь имеет доступ. Доступ к сайтам, не включенным в этот список, заблокирован.

• Список блокировок: этот список содержит сайты, к которым у пользователя нет доступа. Доступ пользователя ко всем другим сайтам разрешен.

1. Откройте стартовый экран продукта, затем **«Настройки защиты»**, далее найдите модуль **«Родительский контроль»**. Затем нажмите на кнопку **«Настройки»** модуля **«Родительский контроль».**

2. Откроется диалоговое окно настроек модуля **«Родительский контроль»** затем выберите вкладку **«Веб фильтр»**.

Для настройки белых списков:

В диалоговом окне **«Веб-фильтр»** выберите вкладку Заблокированные веб-сайты Разрешенные сайты.

Введите доменное имя веб-сайта и нажмите +. Веб-сайт будет добавлен в список.

4. Для удаления веб-сайта выберите его в списке и нажмите .

5. Нажмите **«Закрыть»** для закрытия диалогового окна.

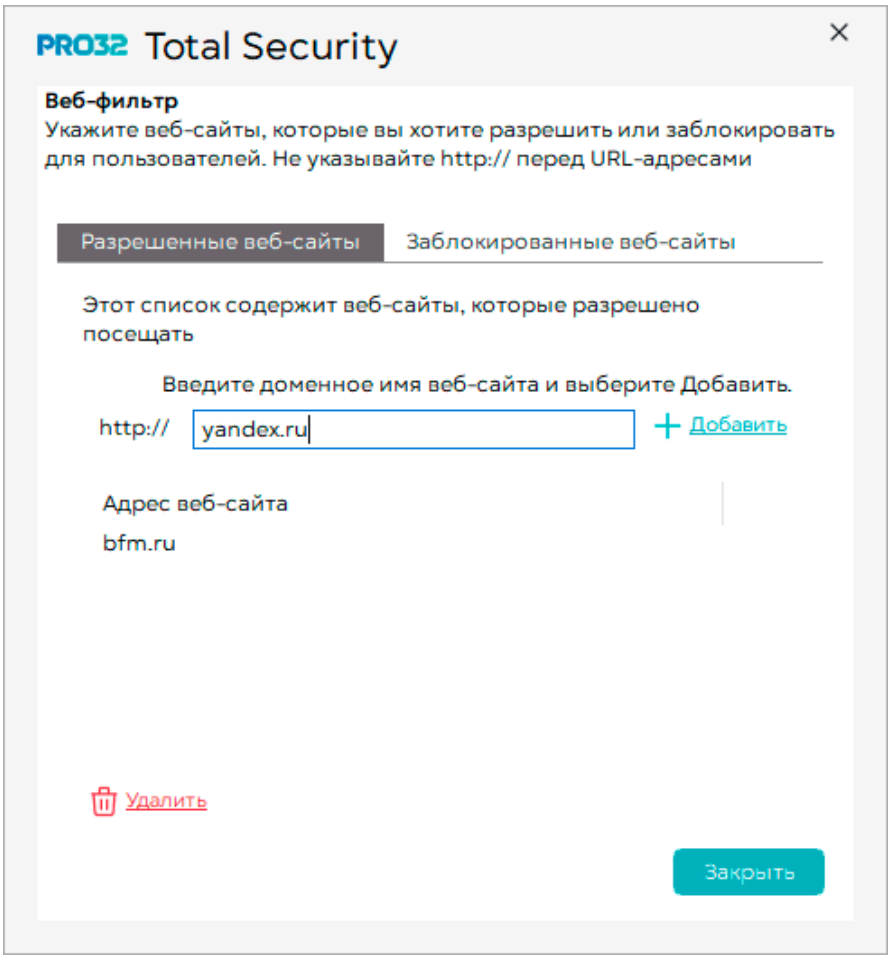
Для настройки списка блокировки:

В диалоговом окне **«Веб-фильтр»** выберите вкладку Заблокированные веб-сайты.

6. Для добавления сайтов в список блокировки введите доменное имя веб-сайта и нажмите . Веб-сайт будет добавлен в список.

7. Для удаления веб-сайта выберите его в списке и нажмите .

8. Нажмите **«Закрыть»** для закрытия диалогового окна.

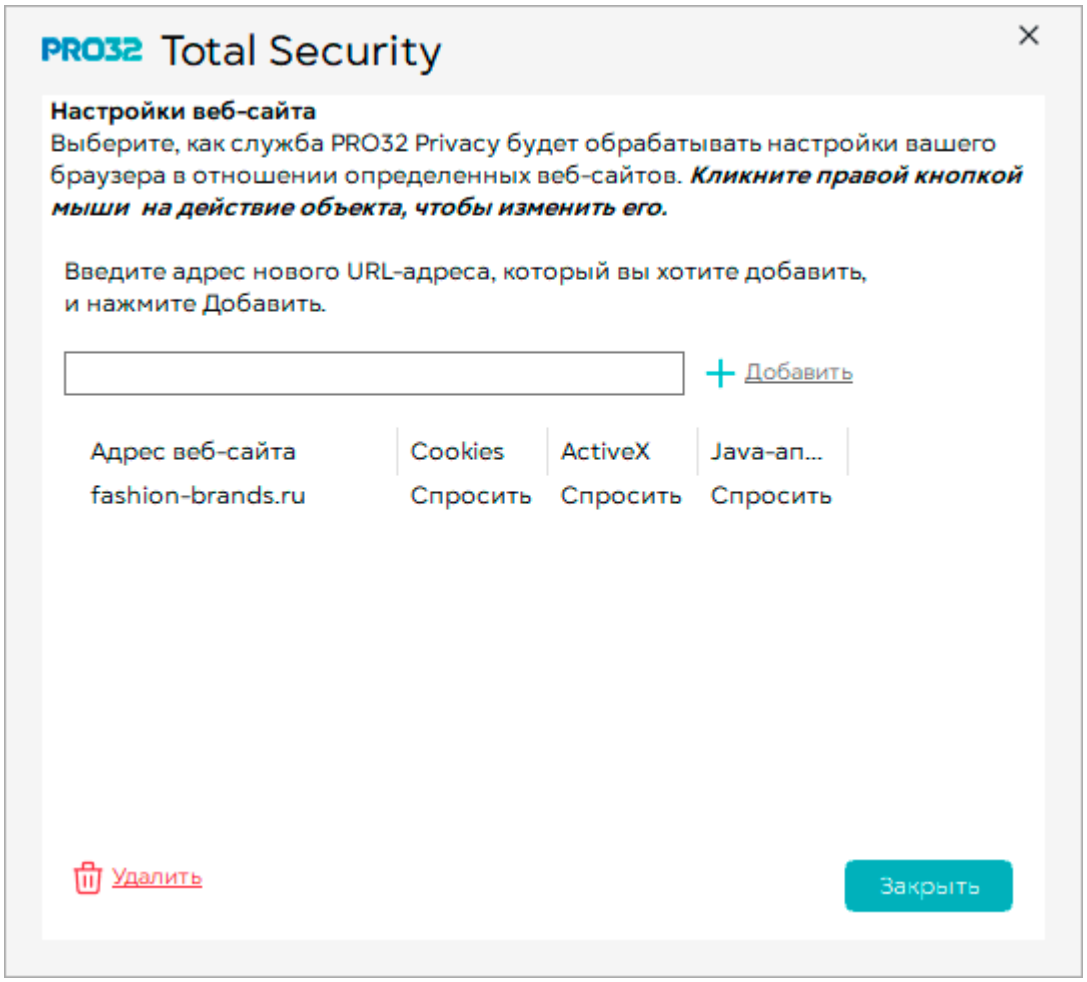


11.3. Настройка параметров браузера

Вы можете настроить доступ к различным сайтам таким образом, чтобы разрешать, блокировать доступ либо отображать запрос в тех случаях, когда веб-сайты, к которым вы обращаетесь, содержат элементы управления ActiveX, файлы cookie или Java-апплеты.

1. Откройте стартовый экран продукта , затем **«Настройки защиты»**, далее найдите модуль **«Родительский контроль»** . Затем нажмите на кнопку **«Настройки»** модуля **«Родительский контроль».**

2. Откроется диалоговое окно настроек модуля **«Родительский контроль»** затем выберите вкладку **«Настройки браузера»** . Откроется диалоговое окно «Настройки веб-сайта».



3. Введите адрес или URL сайта, для которого вы хотите настроить параметры, и нажмите + . Веб-сайт будет добавлен в список.

4. Вы можете настроить действие, предпринимаемое при загрузке файлов cookie, элементов управления ActiveX и Java-апплетов с веб-сайта на ваш компьютер, а также при отправке информации о конфиденциальности на этот веб-сайт с вашего компьютера. По умолчанию система устанавливает вариант **«Запрашивать действие для всех параметров».**

5. Чтобы изменить действие для параметра, щелкните правой кнопкой мыши нужную ячейку и выберите требуемое действие в появившемся контекстном меню. Вы можете разрешить загрузку, заблокировать загрузку или настроить запрос действия при загрузке на ваш компьютер файлов cookie, апплетов Java и элементов управления ActiveX.

6. Для удаления веб-сайта выберите его в списке и нажмите 🗑 .

7. Нажмите **«Закрыть»** для закрытия диалогового окна настроек веб-сайта.

11.4. Настройка ключевых слов для блокировки рекламы

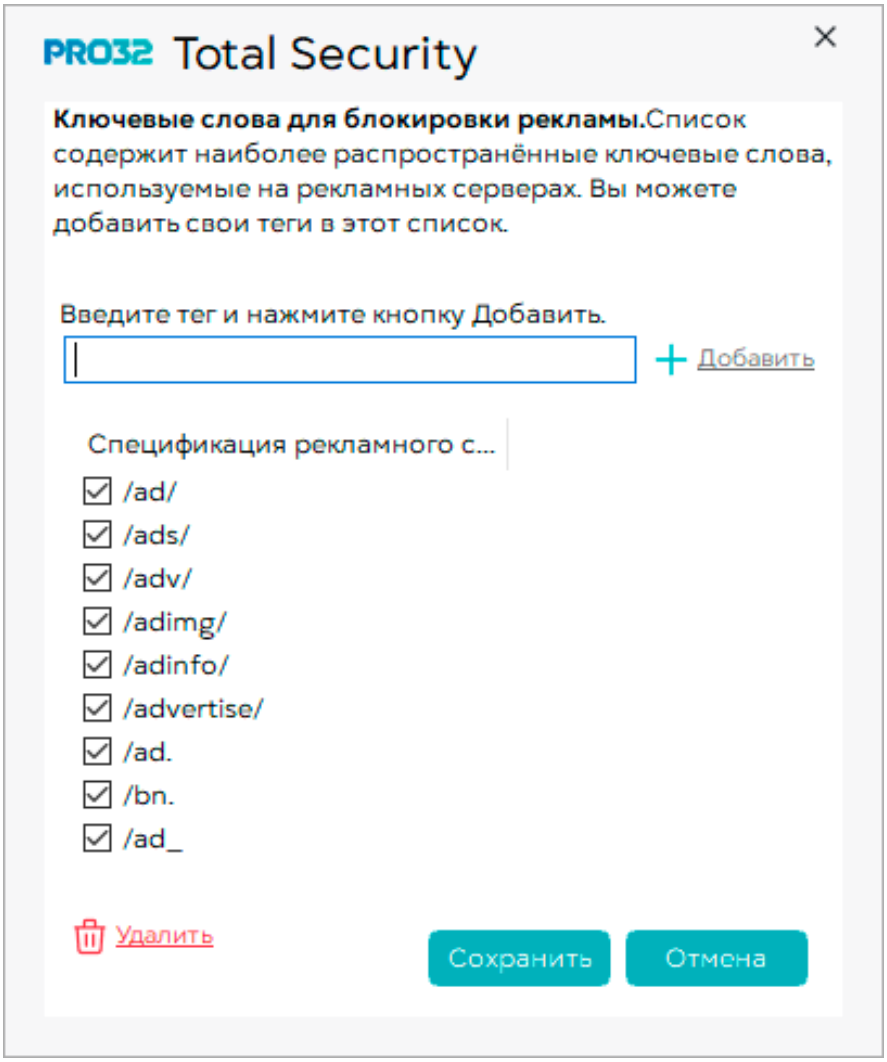
Модуль родительского контроля PRO32 включает в себя список ключевых слов для наиболее распространенных рекламных баннеров на веб-сайтах. Вы можете контролировать рекламу, отображаемую на вашем компьютере при доступе к веб-сайтам, добавляя в этот список текстовые строки, идентифицирующие рекламные баннеры. Строки блокировки рекламы – это разделы

HTML-адресов.

Если блокировка рекламы включена, то при совпадении какой-либо части адреса файла URL с адресом в списке показ рекламы будет заблокирован.

1. Откройте стартовый экран продукта , затем **«Настройки защиты»**, далее найдите модуль **«Родительский контроль»** . Затем нажмите на кнопку **«Настройки»** модуля **«Родительский контроль».**

2. Откроется диалоговое окно настроек модуля **«Родительский контроль»** затем выберите вкладку **«Список рекламных серверов»** . Откроется диалоговое окно «**Ключевые слова для блокировки рекламы**».



4. Введите строку URL-адреса для идентификации рекламных баннеров в отведенном поле и нажмите . Новый тег будет добавлен в список. Когда рекламные объявления соответствуют этим строкам, они блокируются.

5. Для удаления тега выберите его в списке и нажмите .

6. Нажмите **«Сохранить»** для сохранения тегов и закрытия диалогового окна «**Ключевые слова для блокировки рекламы**».

11.5. Настройка управления приложениями

Доступ к приложениям можно ограничить. Заблокированные приложения: этот список содержит приложения, к которым пользователь **не может** получать доступ. Пользователь может запускать все остальные приложения.

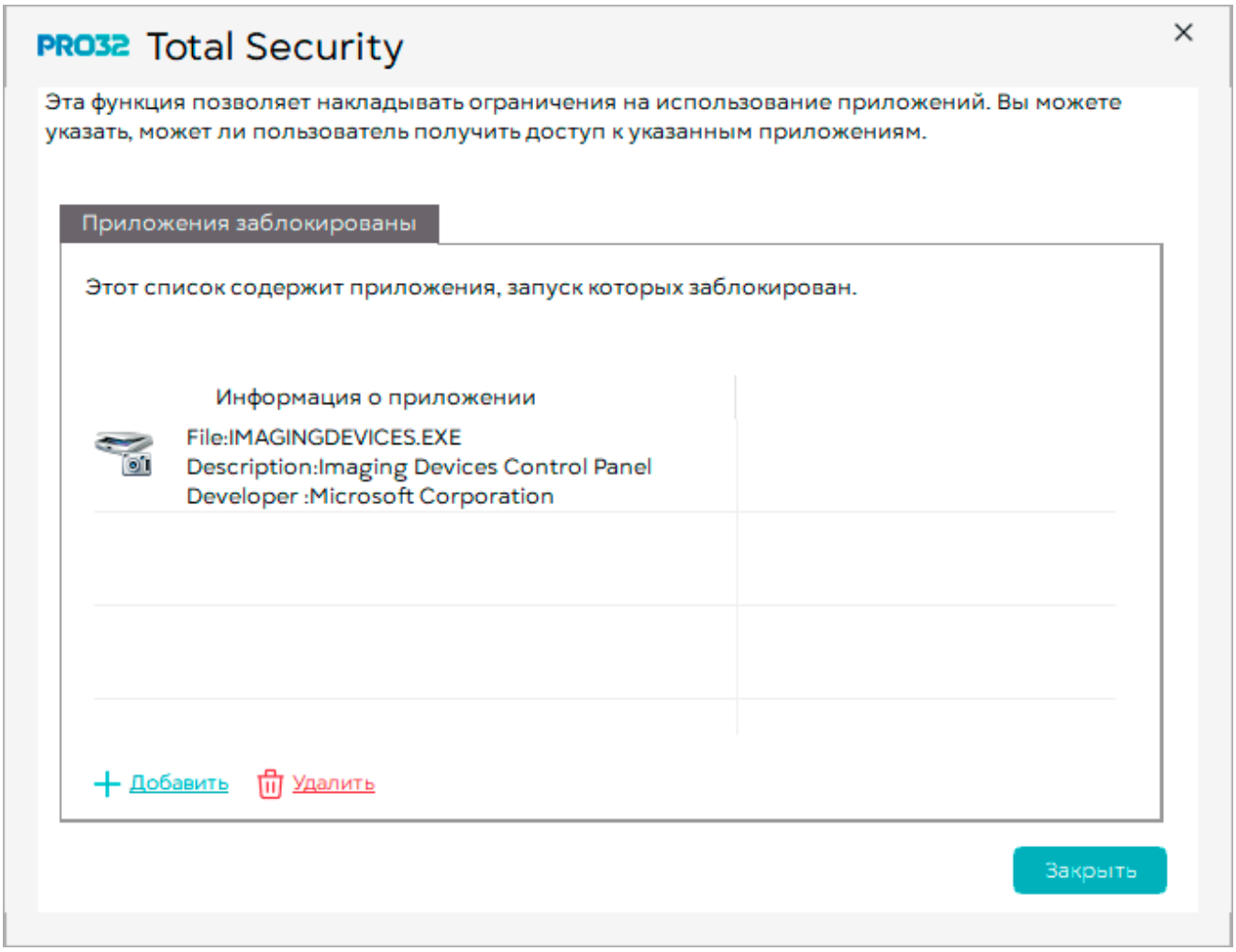
Для настройки списка блокировки:

1.В диалоговом окне «Контроль приложений» перейдите на вкладку Заблокированные приложения.

2. Чтобы добавить приложения в список заблокированных, нажмите +, укажите исполняемый файл и добавьте в список

3. Для удаления веб-сайта выберите его в списке и нажмите .

4. Нажмите **«Закрыть»** для закрытия диалогового окна **«Контроль приложений».**

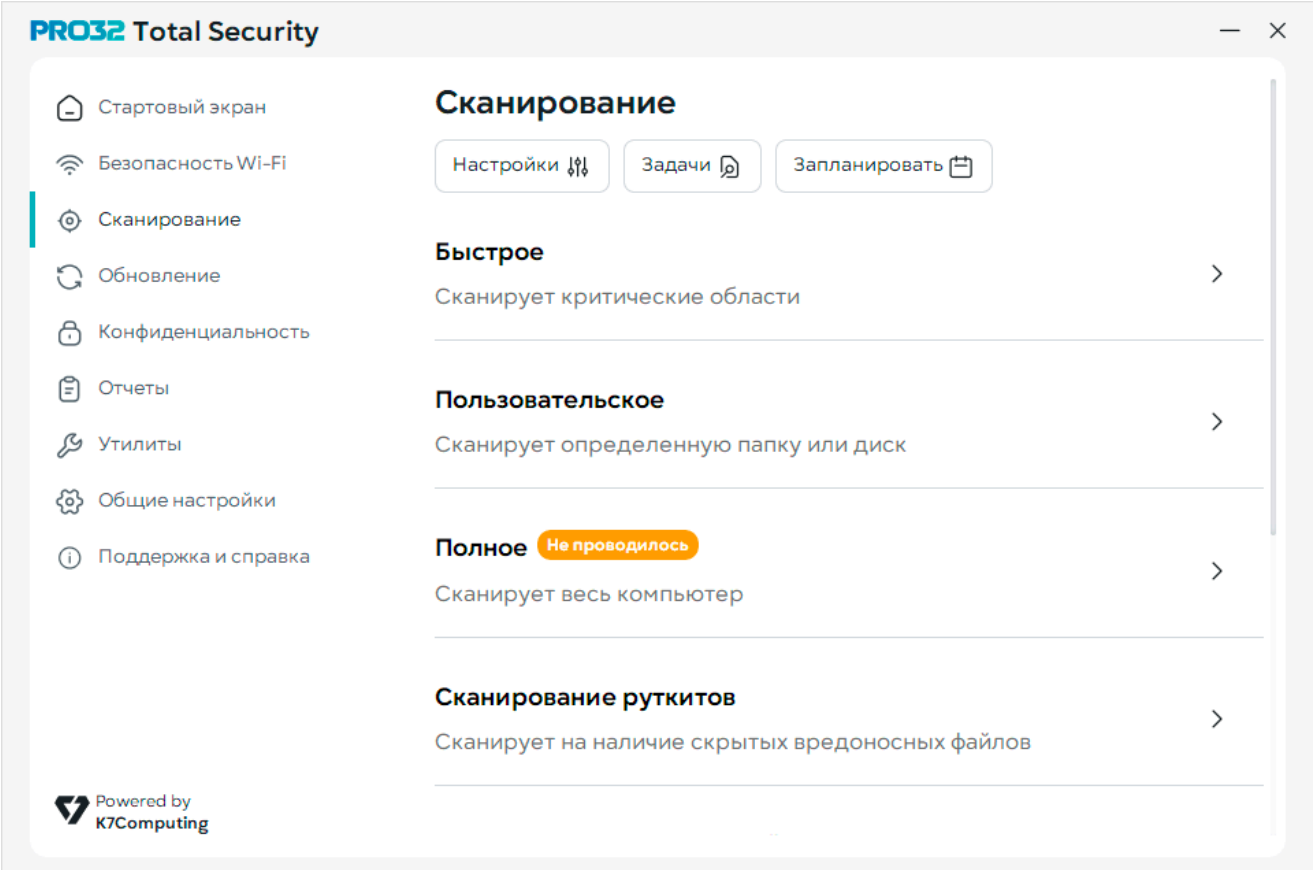


12. Сканирование компьютера

PRO32 Total Security непрерывно проверяет вашу систему в фоновом режиме. Также вы можете запускать собственные проверки/сканирования. Такие сканирования позволяют получить подробную информацию об отсканированных элементах. Вы можете просматривать общее количество просканированных файлов, общее количество обнаруженных вирусов/рисков, а также общее количество устраненных проблем.

Вы можете выбрать одно из следующих действий:

- Выполнить быстрое сканирование
- Выполнить сканирование руткитов
- Выполнить сканирование отслеживающих файлов cookie
- Сканировать всю систему
- Сканировать файл
- Сканировать папку
- Сканировать систему на уязвимости
- Сканировать систему на аномальные изменения



Кнопка **«Настройки»** дублирует функционал, описанный в пунктах 5.1 и 5.1.1 текущего документа.

12.1. Настройка задач сканирования

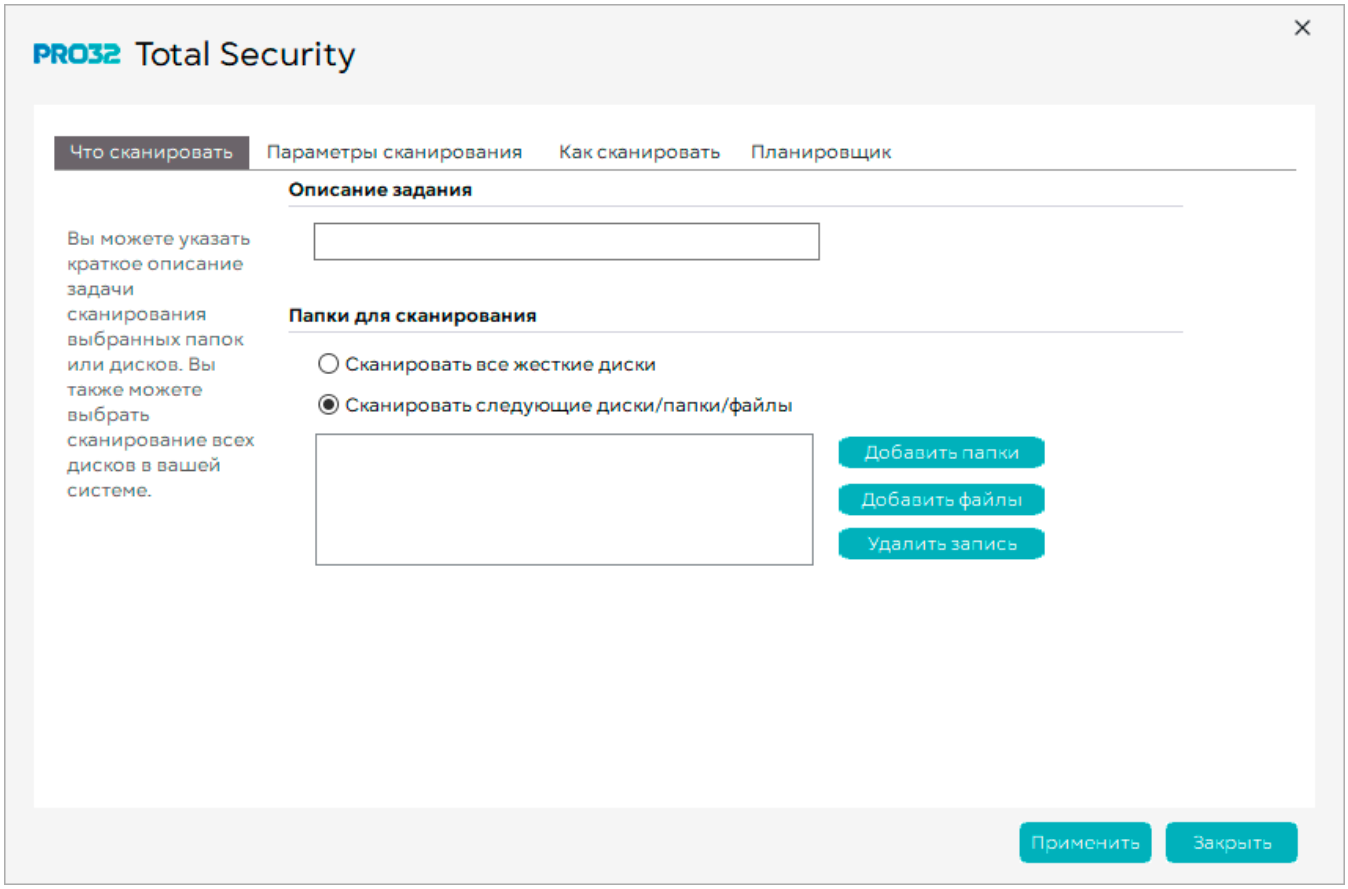
PRO32 Total Security выполняет сканирование всех файлов, к которым обращаетесь вы или ваш компьютер. Вы также можете запланировать автоматическое сканирование компьютера, чтобы проверять его на наличие вирусов и потенциальных угроз через определенные промежутки времени. Некоторые задачи сканирования предустановлены вместе с приобретаемым продуктом, и вам необходимо будет назначить для них расписание. Вы можете создавать и планировать настраиваемые задачи, а также планировать автоматический запуск предопределенных задач в заданное время.

Для настройки задач сканирования

1. Откройте стартовый экран продукта , далее найдите **«Сканирование»** в боковом меню, затем найдите кнопку **«Задачи»** .

2. Откроется диалоговое окно настроек модуля **«Планировщика сканирования».**

3. Выберите вкладку **«Что сканировать».**



Параметры описаны в следующей таблице:

Параметр	Описание
Описание задачи	Название задачи сканирования
Сканирование всех жестких дисков	Сканирует таблицу разделов, загрузочный сектор, а также все файлы на всех жестких дисках вашего компьютера.
Сканировать следующие диски/папки/файлы	Сканирует указанные диски, папки и файлы. Для добавления папок нажмите кнопку «**Добавить папки»** и выберите папку. Для добавления файлов нажмите кнопку **«Добавить файлы»** и найдите файлы, которые вы хотите отсканировать. Для удаления любой из выбранных папок файлов, выберите ее в списке и нажмите **«Удалить запись»**.

4. На вкладке **«Параметры сканирования»** выберите способ сканирования выбранных файлов и папок.

Все файлы

Сканирует все файлы в системе независимо от их расширения или типа

Автоматическое определение

Сканирует все исполняемые (программные) файлы, файлы документов Microsoft и файлы сценариев независимо от того, указаны ли их расширения. Нажмите «Настроить» рядом с этим параметром, чтобы выбрать типы файлов для сканирования.

Заданные расширения

Сканирует файлы с указанными расширениями. Чтобы указать расширение, нажмите пункт Настроить, отображаемый рядом с расширением. Можно просматривать, добавлять или удалять сканируемые расширения.

Выполнять сканирование в архивах

Сканирует файлы в архивах на наличие вирусов и угроз

Обнаружение шпионского и рекламного ПО

Сканирует выбранные файлы на наличие дополнительных угроз, включая шпионское ПО, рекламное ПО, дозвонщики и т. д. Установите флажок, а затем щелкните пункт настроить, который появляется рядом с ним, чтобы настроить тип сканируемых угроз и действие, которое необходимо предпринять при обнаружении угрозы.

Память

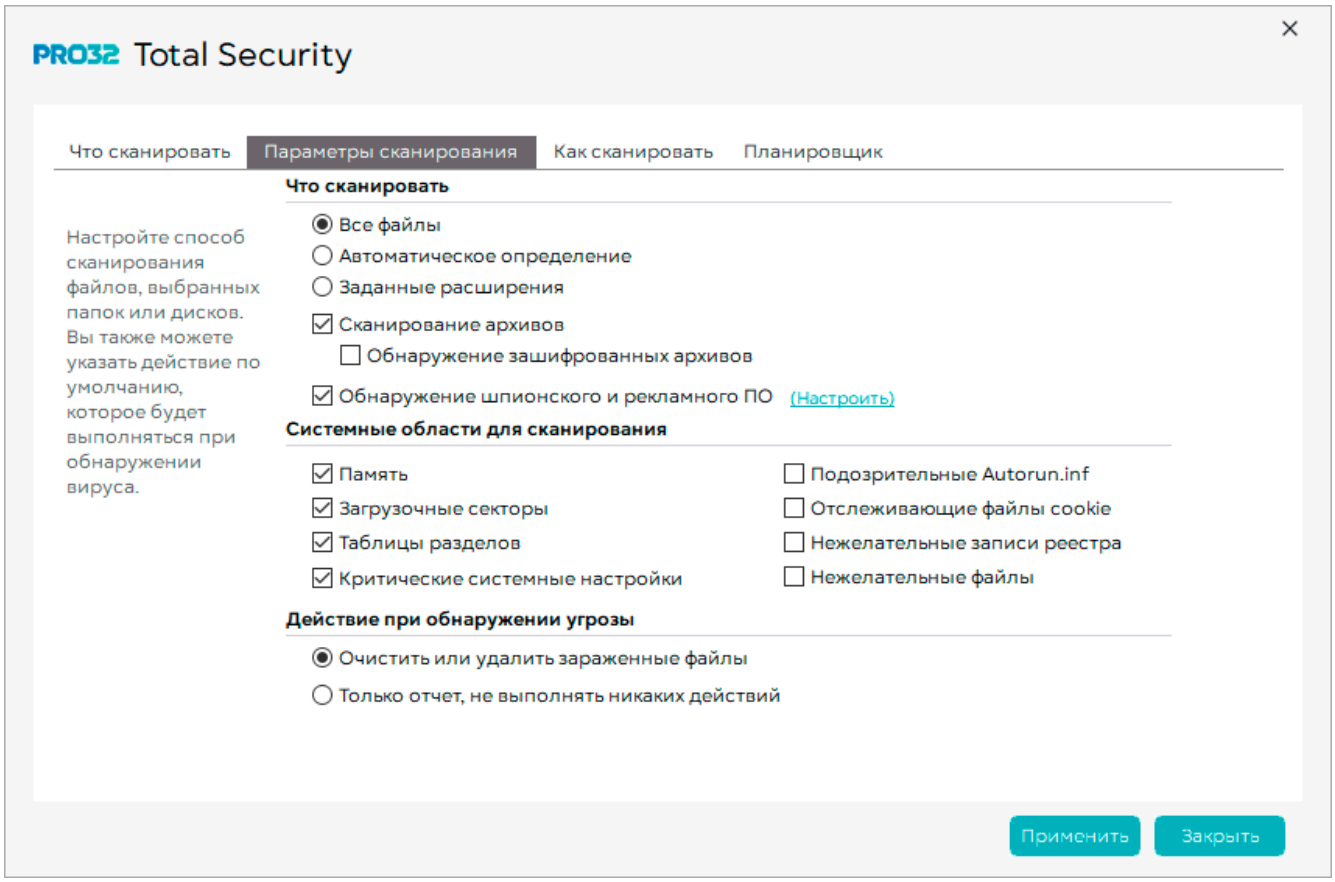
Проверяет память вашего компьютера на наличие вирусов

Загрузочные секторы

Проверяет наличие загружаемых вирусов в загрузочных секторах сканируемого жесткого диска или дискеты.

Таблицы разделов

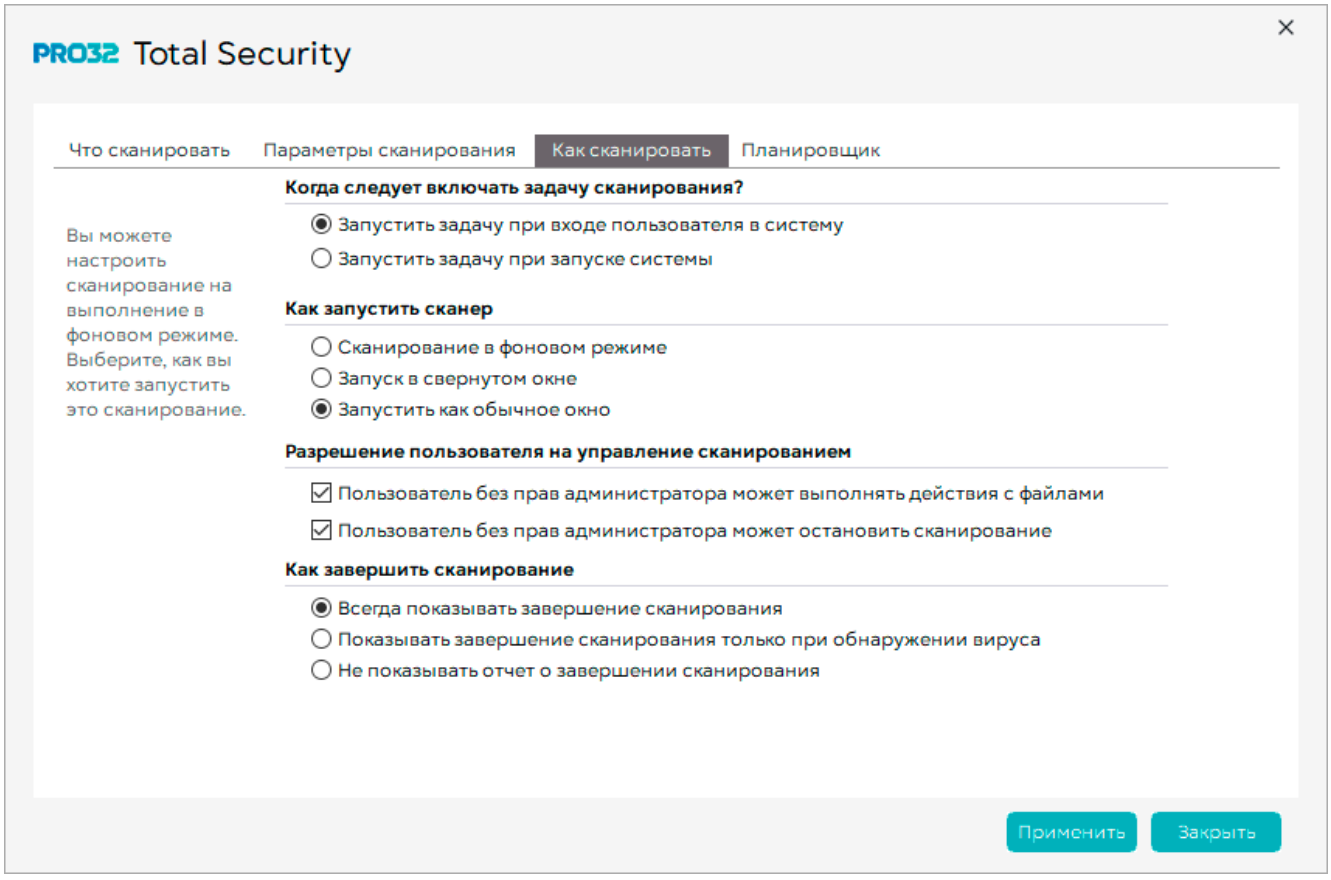
Проверяет наличие вирусов в таблице разделов жесткого диска



5. На вкладке **«Как сканировать»** воспользуйтесь параметрами на панели **«Когда включать задачу сканирования»**.

Параметры описаны в следующей таблице:

Параметр	Описание
Включать задачу только тогда, когда один или несколько пользователей вошли в систему	Включает задачу сканирования *только* тогда, когда один или несколько пользователей вошли в систему компьютера
Включать задачу только независимо от того, вошел ли пользователь в систему	Всегда включает задачу сканирования, даже если пользователь не выполнил вход в систему на компьютере



6. На вкладке **«Как сканировать»** воспользуйтесь параметрами на панели **«Как запускать сканер».** Параметры описаны в следующей таблице:

Параметр	Описание
Сканирование в фоновом режиме	Запускает задачу сканирования в фоновом режиме, не мешая вашей работе
Запустить в свернутом окне	Запускает задачу сканирования со свернутым окном задачи, которое можно открыть в любой момент для просмотра состояния сканирования.
Запустить в обычном окне	Запускает задачу сканирования в окне, отображаемом во время проверки.

7. Для настройки действий, которые пользователь может выполнять с задачей сканирования, используйте параметры на панели **«Разрешение пользователя на управление сканированием»**. Параметры описаны в следующей таблице:

Параметр	Описание
Пользователь без прав администратора может выполнять действия с файлами из отчетов	Выберите этот параметр, если вы хотите разрешить пользователю, не имеющему прав администратора, выполнять действия с файлами, которые, как указано в отчетах, содержат вирусы или представляют собой потенциальную угрозу.
Пользователь без прав администратора может останавливать сканирование	Выберите этот параметр, чтобы разрешить пользователю без прав администратора останавливать сканирование в процессе его выполнения.

8. Для выбора способа завершения сканирования выберите параметр на панели **«Как завершать сканирование»**. Параметры описаны в следующей таблице.

Параметр	Описание
Всегда показывать завершение сканирования	Отображает окно «Сводка сканирования» после завершения задачи сканирования, независимо от того, обнаружен ли вирус.
Показывать завершение сканирования только при обнаружении вируса	Отображает окно «Сводка сканирования» после завершения задачи сканирования, в результате которой был обнаружен вирус. Если вирус не обнаружен, сообщение о завершении сканирования не выводится.
Не отображать отчет о завершении сканирования	Выберите этот вариант, чтобы не выводить отчет о завершении сканирования.

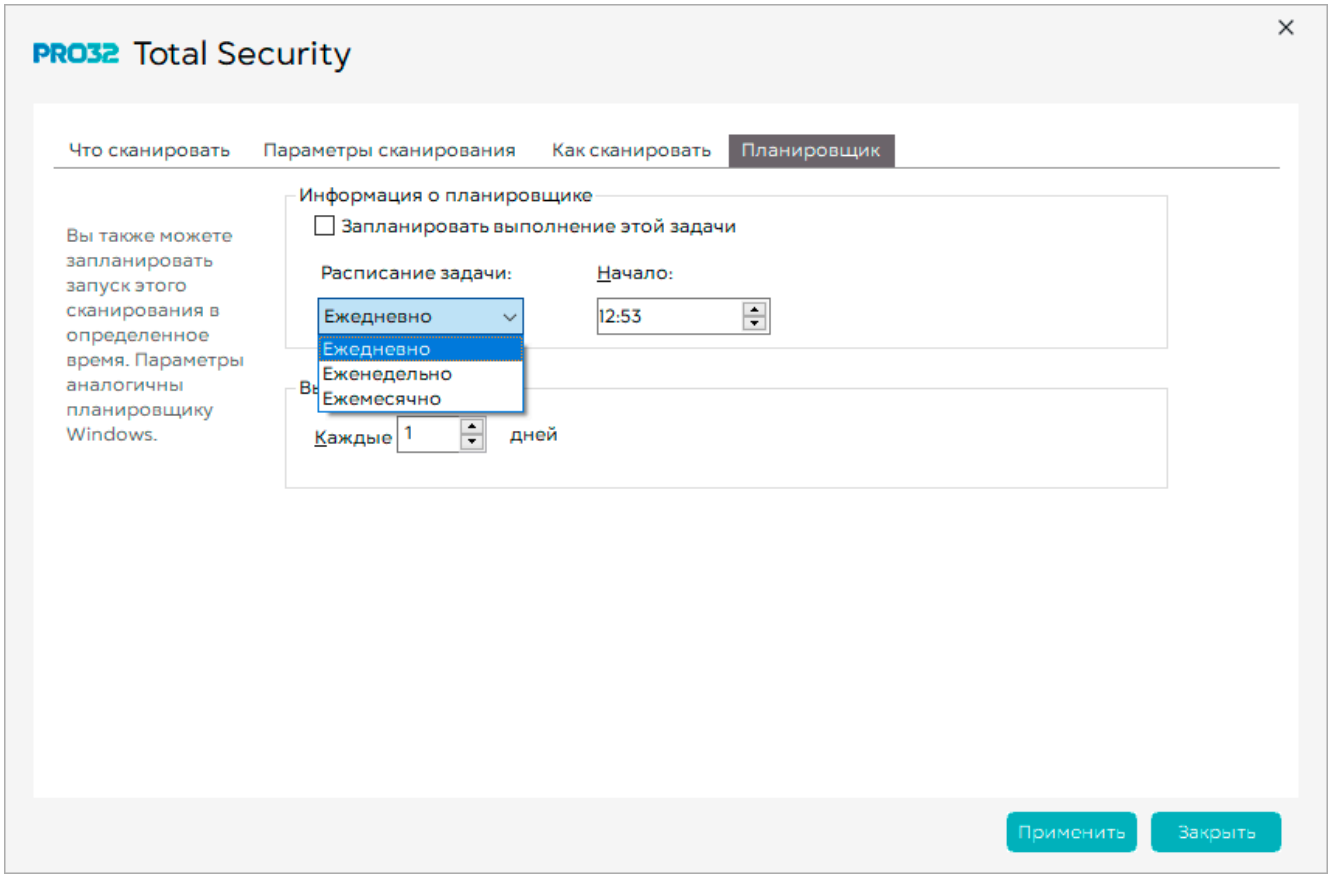
3. Нажмите **«Применить»** для сохранения параметров сканирования.

Для настройки расписания сканирования

1. Откройте стартовый экран продукта, далее найдите **«Сканирование»** в боковом меню, затем найдите кнопку **«Задачи»**.

2. Откроется диалоговое окно настроек модуля **«Планировщика сканирования».**

3. Выберите вкладку **«Планировщик».**



4. Выберите периодичность, с которой требуется запускать задачу, в раскрывающемся списке Расписание задачи. Вы можете запланировать выполнение задачи каждый день, в определенные дни недели или в любой день месяца. Параметры на панели ниже отображаются в соответствии с выбранной периодичностью.

5. Используйте элементы управления Время запуска, чтобы установить время суток для выполнения задачи.

6. Выберите периодичность запуска сканирования на панели **«Планировщик»** и задайте дополнительные параметры, которые отображаются на панели, в зависимости от вашего выбора. Варианты, отображаемые в зависимости от вашего выбора:

• Ежедневно – укажите количество дней между проверками на панели «**Запланировать задачу ежедневно».**

• Еженедельно – укажите количество недель между сканированиями и дни недели для запуска сканирования на панели **«Запланировать задачу еженедельно».**

• Ежемесячно– укажите день месяца для выполнения задачи сканирования на панели **«Запланировать задачу ежемесячно».**

7. Нажмите кнопку Применить для сохранения расписания.

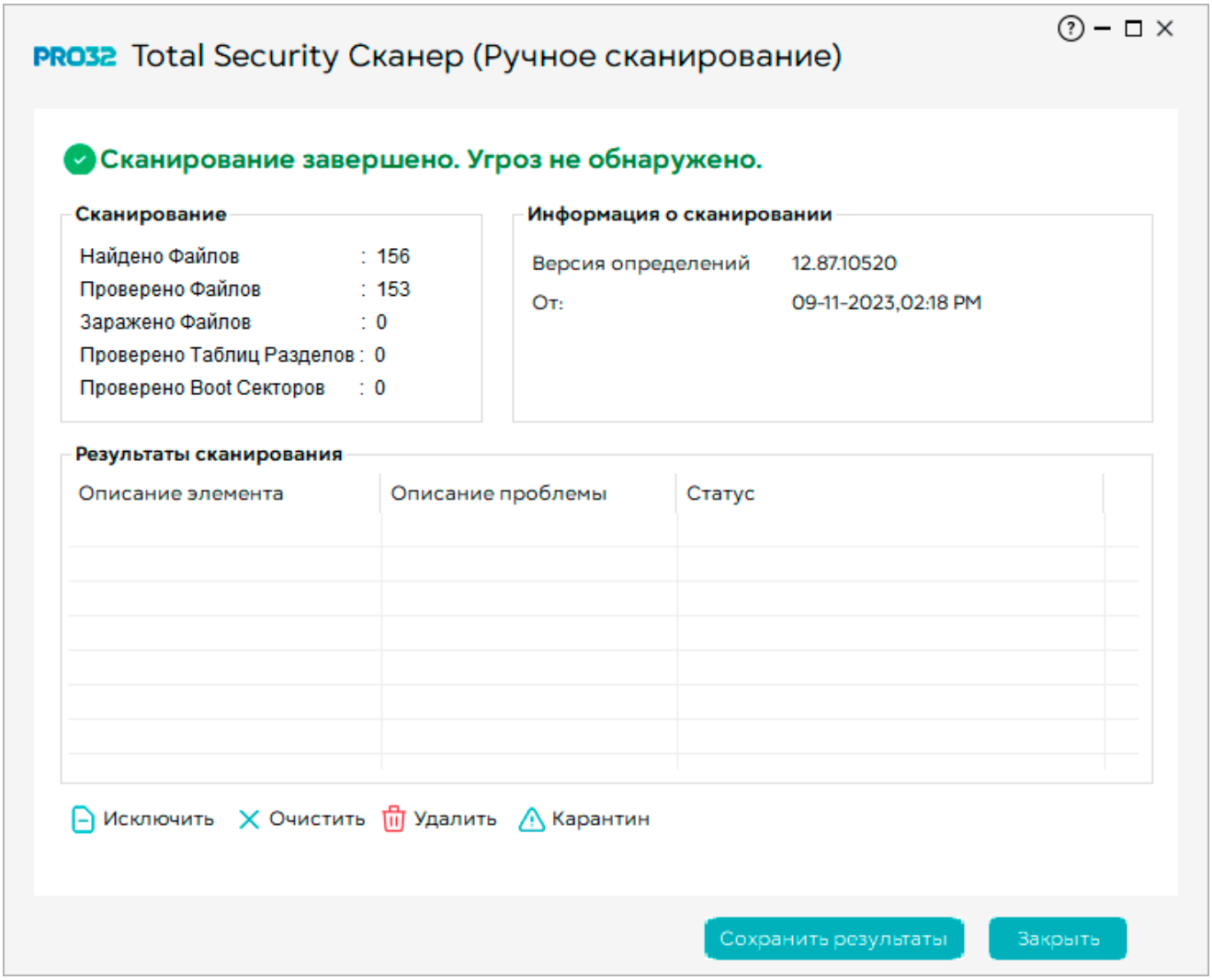
8. Нажмите кнопку Закрыть для закрытия диалогового окна **«Планировщик».**

12.2. Выполнение быстрого сканирования

Быстрое сканирование предназначается для проверки дисков и папок (то есть папок диска C,Windows и ProgramFiles) на вашем компьютере на наличие вирусов и других потенциальных угроз.

1. Откройте стартовый экран продукта , далее найдите **«Сканирование»** в боковом меню, затем найдите кнопку **«Быстрое сканирование»** .

2. Продукт начнёт сканирование и откроется соответствующее диалоговое окно. Результаты будут отображены на экране.



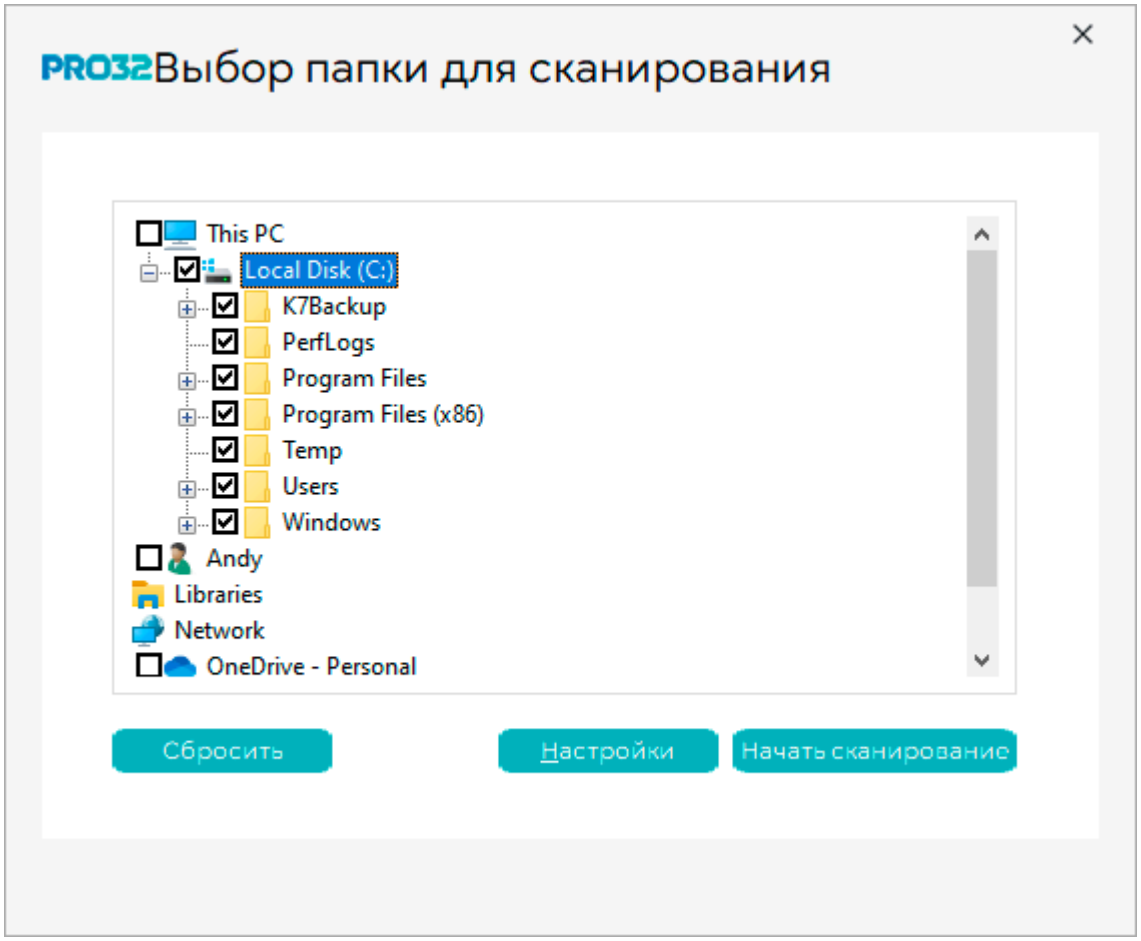
12.3. Выполнение пользовательского сканирования

Если вы хотите вручную отсканировать несколько дисков или папок на вашем компьютере (без сканирования всего компьютера), вы можете указать папки для сканирования.

1. Откройте стартовый экран продукта , далее найдите **«Сканирование»** , в боковом меню, затем найдите кнопку **«Пользовательское сканирование»** .

2. Продукт начнёт сканирование и откроется соответствующее диалоговое окно. Результаты будут отображены на экране.

3. Отображаются папки, доступные на вашем компьютере. Чтобы развернуть папку, нажмите значок «+» значок рядом с ее названием. Значок изменит вид на «-». Нажмите значок «-», чтобы свернуть папку.



4. Установите флажки для папок, которые требуется отсканировать, и нажмите **«Начать сканирование».** Откроется диалоговое окно, показывающее ход сканирования.

5. Выбранная папка будет отсканирована, результат сканирования отобразится в диалоговом окне. Если в выбранных папках обнаружены вирусы, в диалоговом окне будут показаны подробные сведения.

6. Для очистки зараженного файла выберите файл из списка и нажмите **«Очистить»** .

7. Если требуется удалить файл, содержащий вирус, выберите зараженный файл и нажмите **«Удалить»** .

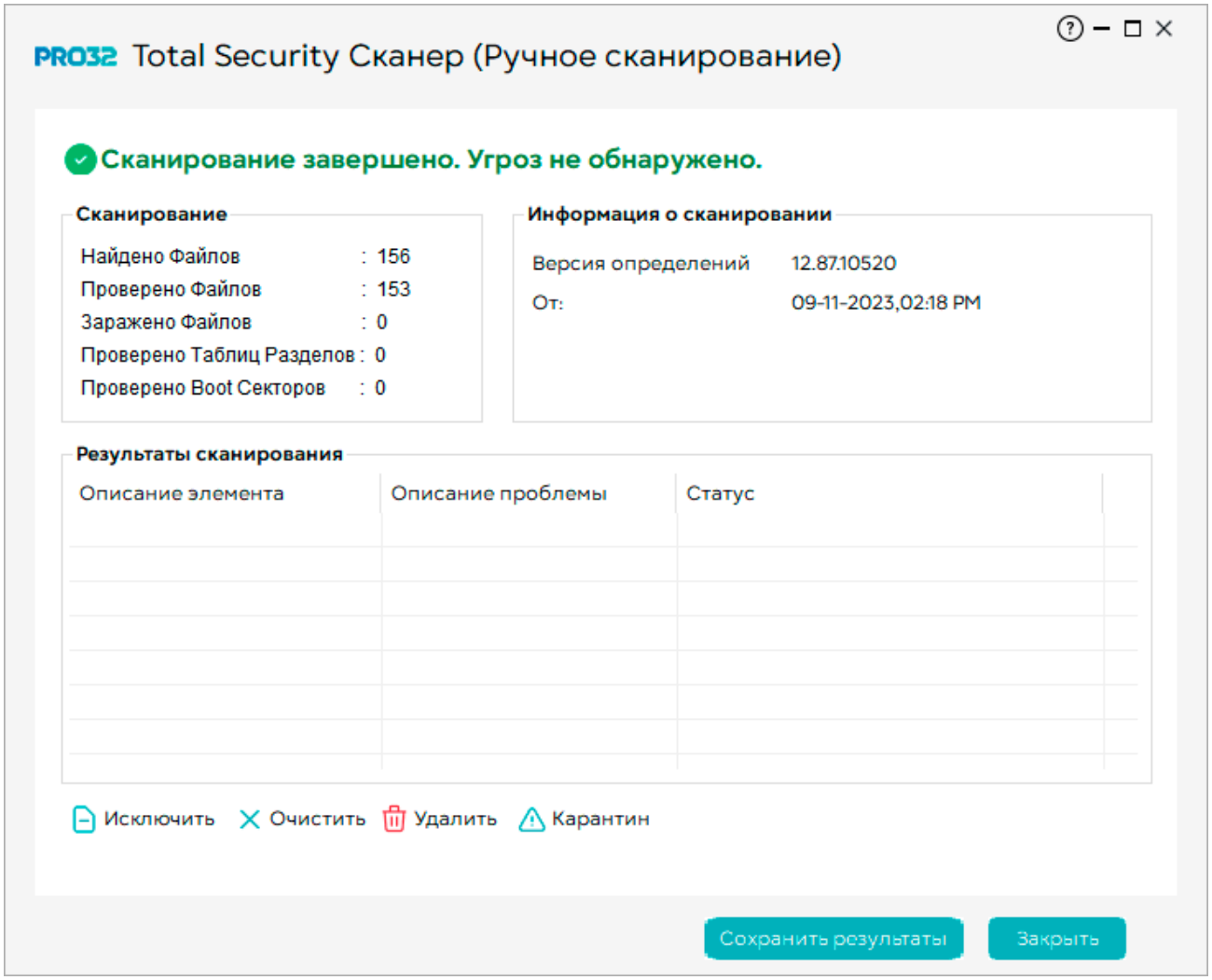
8. Чтобы поместить зараженный файл в карантин, выберите файл в списке и нажмите **«Карантин»** .

9. Если в выбранных папках вирусы не обнаружены, появится сообщение .

10. Нажмите кнопку «**Стоп»** в правом нижнем углу диалогового окна для остановки сканирования. После завершения сканирования параметр изменит вид на **«Закрыть»**.

11. Чтобы настроить параметры сканирования, нажмите кнопку **«Настройки».** Откроется диалоговое окно Настройка защиты от вредоносных программ.

12. Выберите параметры сканирования и нажмите **«Закрыть».** Дополнительные сведения см. в разделе Настройка параметров сканирования.



13. Для сброса настроек сканирования нажмите кнопку **«Сбросить».**

14. Нажмите кнопку **«Закрыть»,** чтобы закрыть диалоговое окно сканера.

12.4. Запуск сканера руткитов

1. Откройте стартовый экран продукта, далее найдите **«Сканирование»**, в боковом меню, затем найдите кнопку **«Полное сканирование»** .

2. Продукт начнёт сканирование и откроется соответствующее диалоговое окно. Результаты будут отображены на экране.

3. Откроется диалоговое окно, показывающее ход сканирования.

4. Будут отсканированы все диски и папки на вашем компьютере, результат сканирования отобразится в диалоговом окне. Сканирование выполняется в соответствии с настроенными параметрами.

5. Если на каком-либо из дисков или папок обнаружены вирусы, в диалоговом окне будут показаны подробные сведения.

6. Чтобы исключить файл, который был определен как зараженный, из лечения и будущих проверок, выберите такой файл в списке и нажмите **«Исключить»** .

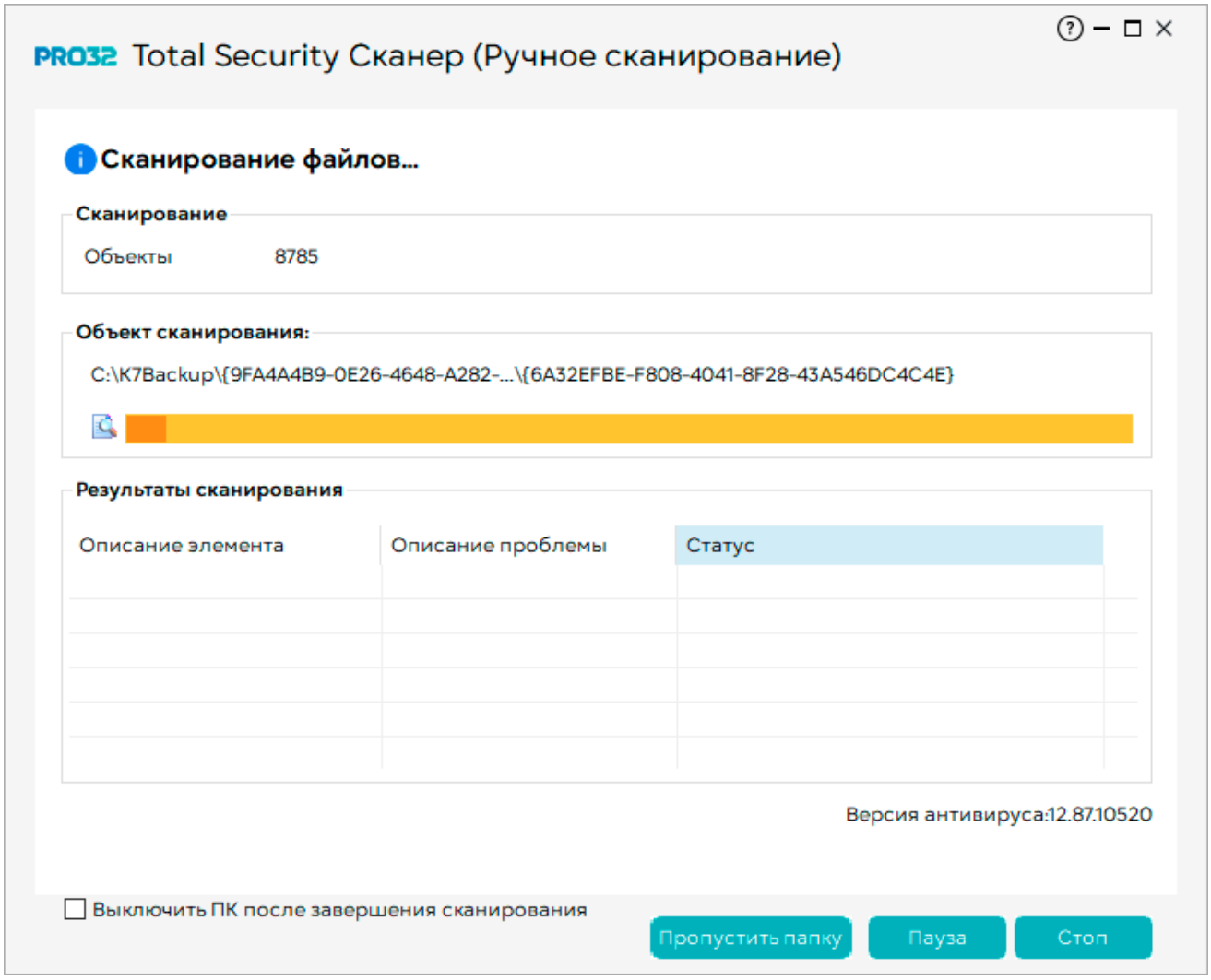
7. Для очистки зараженного файла выберите файл из списка и нажмите **«Очистить»** .

8. Если требуется удалить файл, содержащий вирус, выберите зараженный файл и нажмите

«Удалить» .

9. Чтобы поместить зараженный файл в карантин, выберите файл в списке и нажмите **«Карантин»** .

10. Если в выбранных папках вирусы не обнаружены, появится сообщение .



11. Нажмите кнопку **«Сохранить»** результат для сохранения результата сканирования.

12. Нажмите кнопку **«Закрыть»** в верхней части диалогового окна для остановки сканирования. После завершения сканирования параметр изменит вид на Выход.

13. Вы можете дать команду «**Выключить ПК после завершения сканирования»,** воспользовавшись соответствующим флажком.

12.5. Запуск сканера руткитов

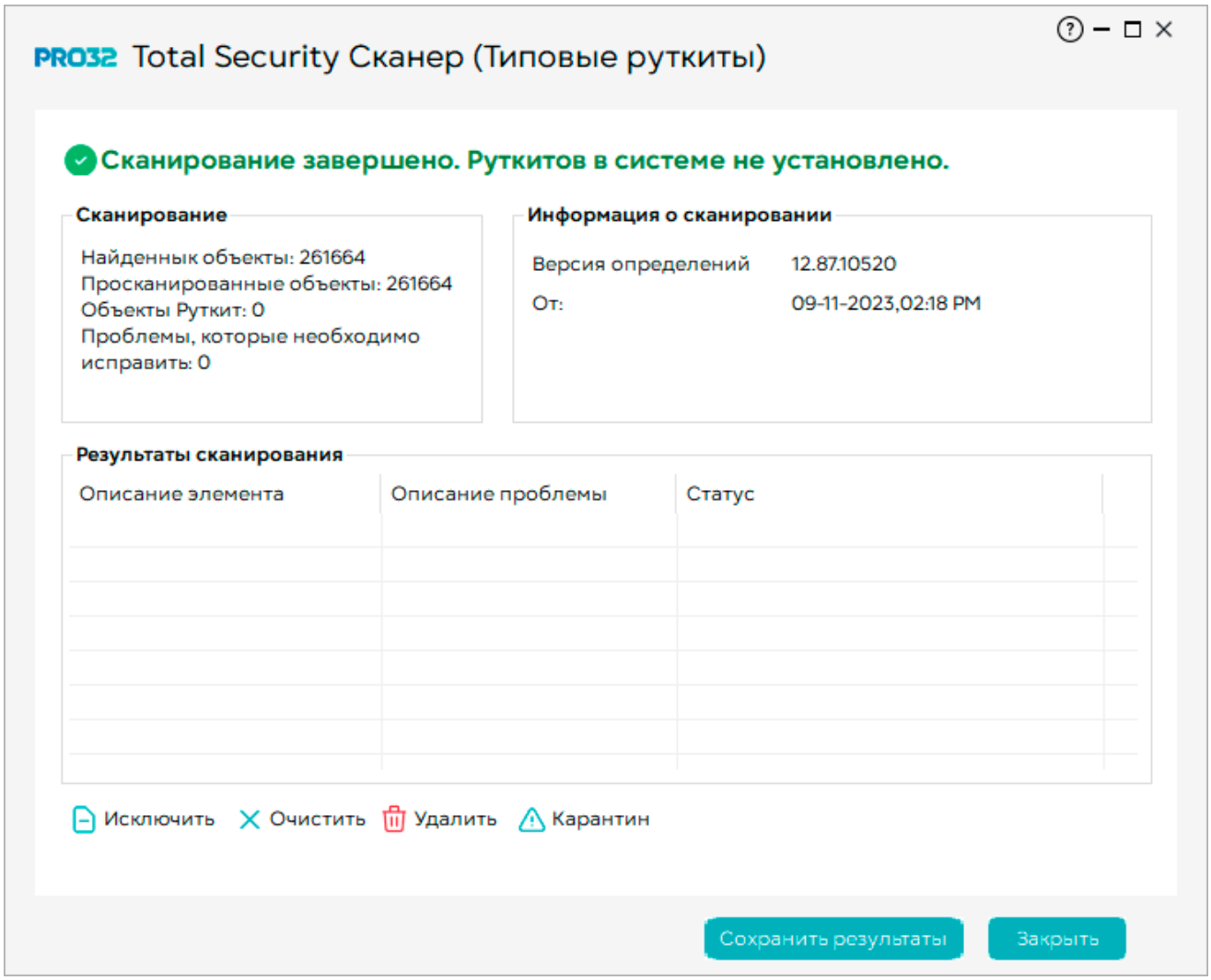
Глубокое сканирование на наличие руткитов можно использовать для общего сканирования системы.

1. Откройте стартовый экран продукта , далее найдите **«Сканирование»** , в боковом меню, затем найдите кнопку **«Сканирование руткитов»** .

2.Продукт начнёт сканирование и откроется соответствующее диалоговое окно. Результаты будут отображены на экране.

3. Откроется диалоговое окно, показывающее ход сканирования.

4. Сканер руткитов проверяет скрытые записи реестра, скрытые процессы и скрытые записи файловой системы. Результат сканирования отобразится в диалоговом окне.



12.6. Сканирование системы на уязвимости

Сканер уязвимостей идентифицирует уязвимости в системе и предлагает шаги по исправлению системы для защиты от таких уязвимостей.

1. Откройте стартовый экран продукта, далее найдите **«Сканирование»** в боковом меню, затем найдите кнопку **«Сканирование уязвимостей»** .

2. Продукт начнёт сканирование и откроется соответствующее диалоговое окно. Результаты будут отображены на экране.

3. Откроется диалоговое окно, показывающее ход сканирования.

4. Если продукт обнаружит уязвимости, в диалоговом окне будут показаны подробные сведения.

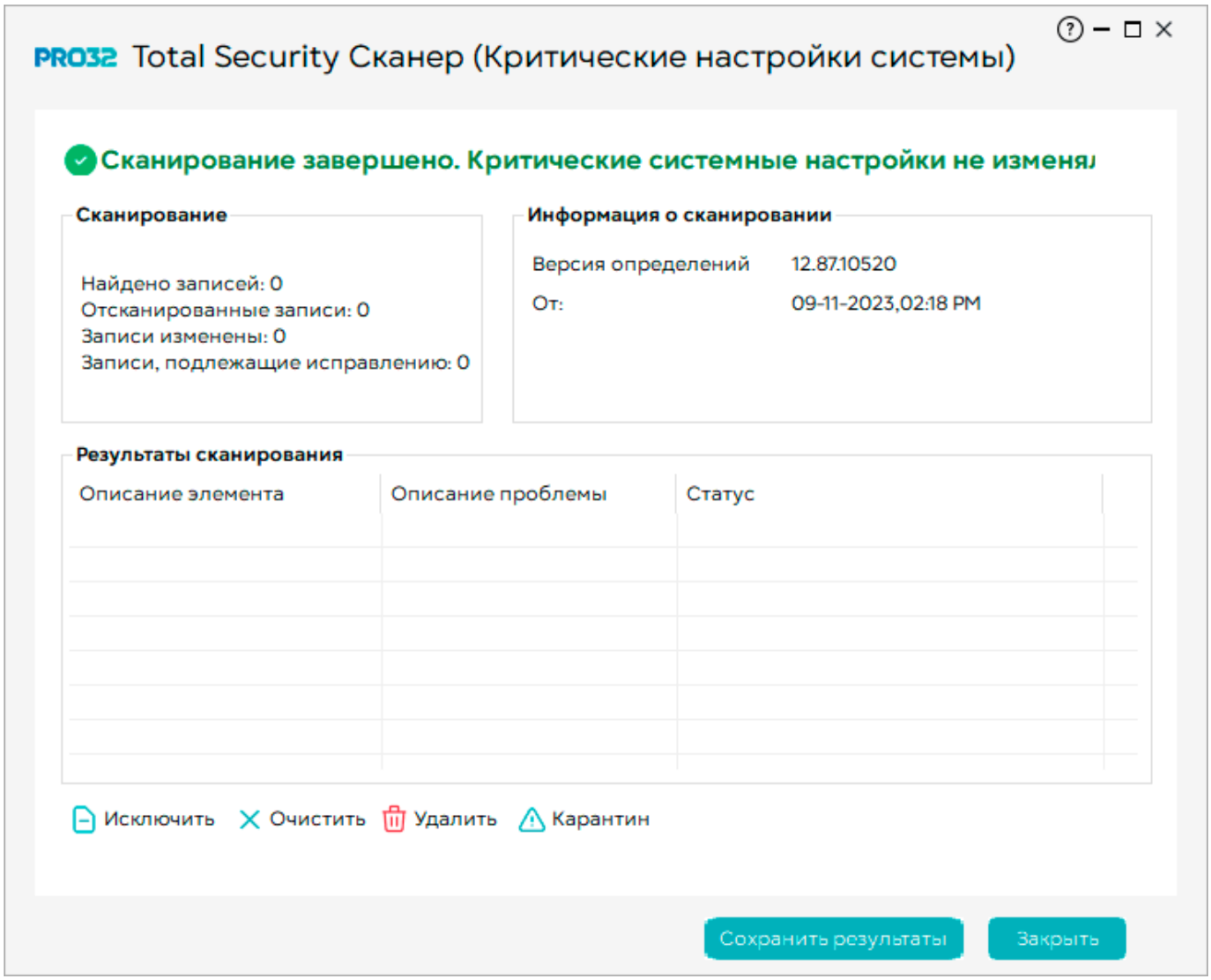
6. Чтобы исключить уязвимость, которая был определена как зараженная, из лечения и будущих проверок, выберите такой файл в списке и нажмите **«Исключить»** .

7. Для очистки зараженного файла выберите файл из списка и нажмите **«Очистить»** .

8. Если требуется удалить файл, содержащий вирус, выберите зараженный файл и нажмите **«Удалить»** .

9. Чтобы поместить зараженный файл в карантин, выберите файл в списке и нажмите **«Карантин»** .

10. Если в выбранных папках вирусы не обнаружены, появится сообщение .



12.6. Сканирование системы на Аномальные изменения

Есть несколько системных настроек, которые имеют определяющее значение для нормального функционирования и безопасности системы. Это сканирование позволяет проверить такие критические изменения реестра.

1. Откройте стартовый экран продукта , далее найдите **«Сканирование»** в боковом меню, затем найдите кнопку **«Аномальные изменения»** .

2. Продукт начнёт сканирование и откроется соответствующее диалоговое окно. Результаты будут отображены на экране.

3. После того, как сканирование будет завершено, результаты сканирования отобразятся в диалоговом окне сканера.

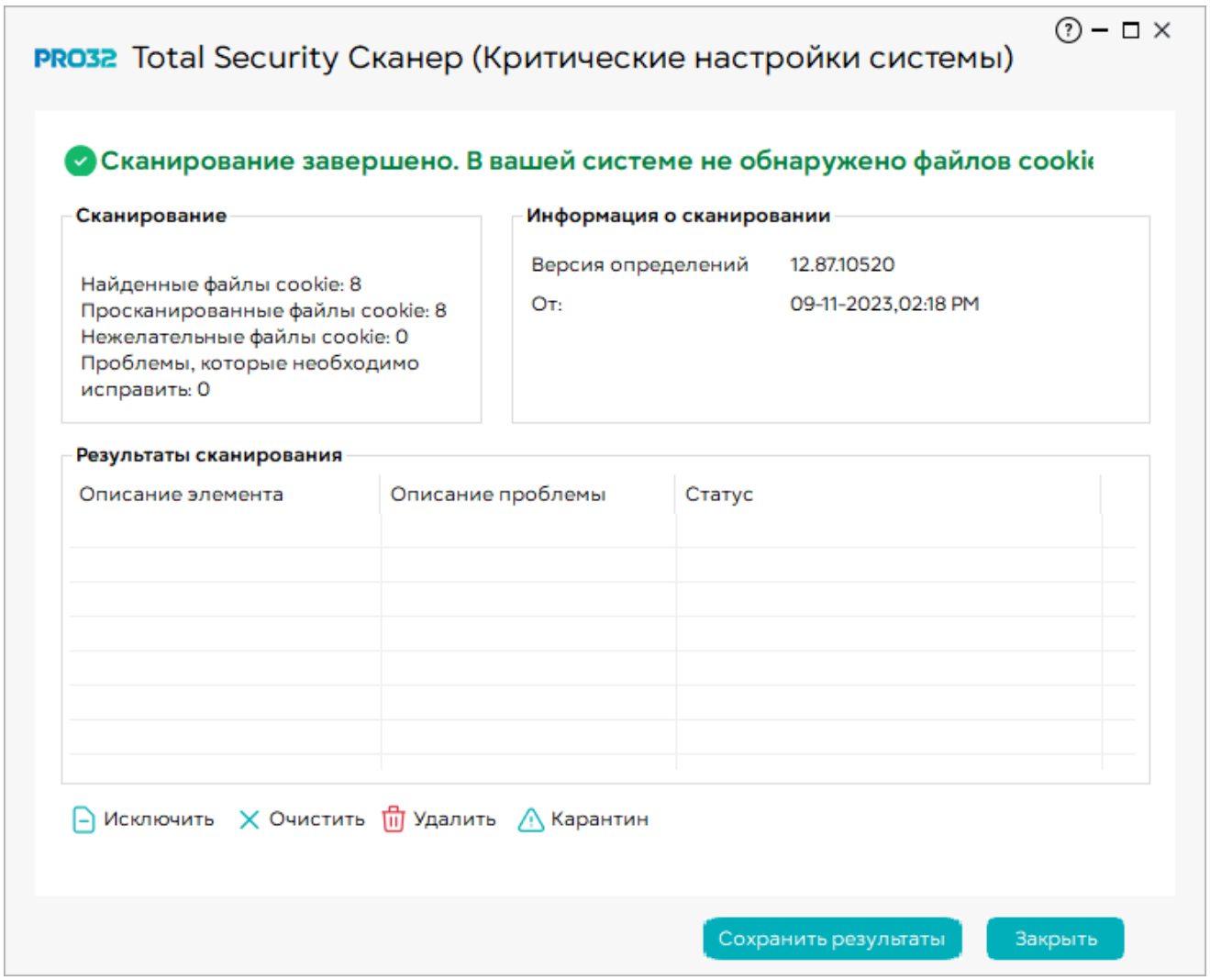
12.7. Запуск сканера для отслеживания файлов cookie

Отслеживающие файлы cookie – это фрагменты информации, сохраняемые на компьютере браузером, которые позволяют веб-сайту однозначно идентифицировать пользователя. Сканирование для обнаружения отслеживающих файлов cookie, присутствующих у текущего пользователя, вошедшего в систему.

1. Откройте стартовый экран продукта , далее найдите **«Сканирование»** в боковом меню, затем найдите кнопку **«отслеживающие файлы cookie»** .

2. Продукт начнёт сканирование и откроется соответствующее диалоговое окно. Результаты будут отображены на экране.

3. После того, как сканирование будет завершено, результаты сканирования отобразятся в диалоговом окне сканера.



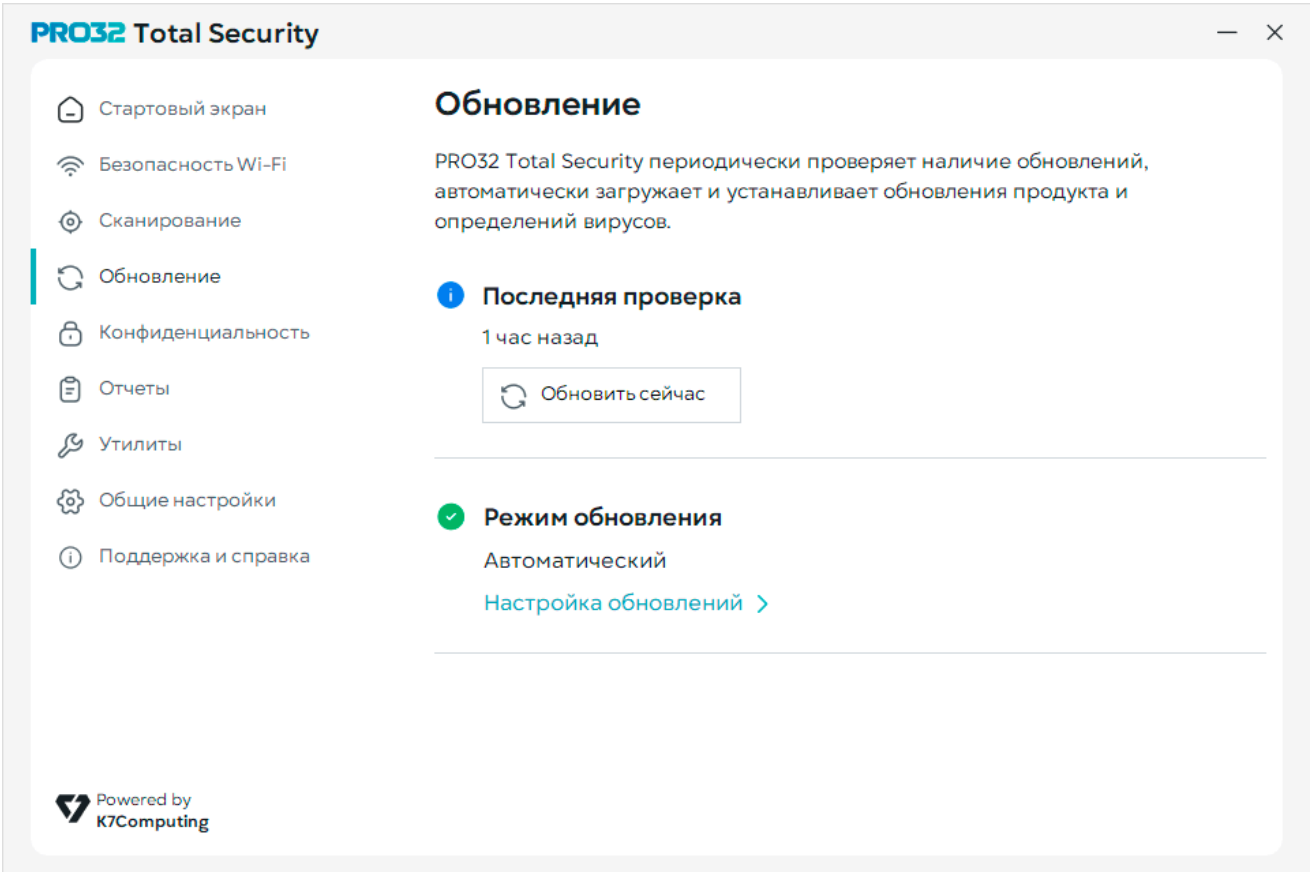
13. Обновление продукта

Для защиты компьютера от недавно обнаруженных вирусов и угроз необходимо постоянно обновлять продукт PRO32 Total Security, установленный на вашем компьютере. Безопасность вашего компьютера напрямую зависит от регулярного обновления сигнатур угроз и программных модулей. Обновления продукта – это усовершенствования **установленного** продукта. Обновления можно получать на веб-сайте PRO32 в течение срока действия вашей лицензии. Когда срок действия вашей лицензии подойдет к концу, вам будет предложено продлить ее.
Перед обновлением продукт должен быть активирован.

PRO32 Total Security автоматически настроен на проверку обновлений при подключении к Интернету, с последующим выводом уведомлений. Вы можете настроить PRO32 Total Security таким образом, чтобы он уведомлял вас перед загрузкой и установкой обновлений.
Для проверки доступных обновлений PRO32 Total Security требуется подключение к Интернету.

Доступны следующие варианты выбора:

- Автоматическая проверка обновлений
- Ручная проверка обновлений
- Отключение автоматической проверки обновлений



13.1. Ручная проверка обновлений

Вы можете в любое время выполнить обновление продукта вручную для использования самой актуальной защиты. Кроме того, рекомендуется выполнять обновление вручную при каждой вспышке угрозы, а также в том случае, если подозреваете, что ваш компьютер заражен, однако сканирование не выявило каких-либо угроз.

1. Откройте стартовый экран продукта, далее найдите **«Обновления»** в боковом меню, затем найдите кнопку **«Настройка обновлений»** .

2. Убедитесь, что вы подключены к Интернету, и нажмите **«Обновить сейчас».** Продукт подключится к веб-сайту PRO32 и загрузит обновления. Будет показано сообщение со статусом обновления.

Для обновления вашего продукта у него должна быть действующая лицензия. Если срок действия лицензии истек, выводится предупреждение.

3. После обновления продукта вам нужно будет закрыть все открытые приложения и перезагрузить компьютер, чтобы обновление вступило в силу.

13.2. Автоматическая проверка обновлений

Вы можете настроить продукт на автоматическую проверку обновлений защиты. Новые обновления публикуются на веб-сайте PRO32. Если вы настроите продукт на автоматическую проверку обновлений, он будет получать новые обновления с веб-сайта PRO32 без вашего вмешательства при наличии подключения к Интернету. Продукт будет проверять наличие обновлений каждые пять минут, а после успешного обновления снова подключится к сайту PRO32 для проверки обновлений через три часа.

Настройка продукта на автоматическую проверку обновлений:

1. Откройте стартовый экран продукта, далее найдите **«Обновления»** в боковом меню, затем найдите кнопку **«Настройка обновлений»** .

2. Нажмите **«Режим обновлений»** .Откроется диалоговое окно **«Менеджер Обновлений».**

3. Установите флажок **«Автоматически проверять наличие обновлений».**

4. Можно выбрать последовательность, в которой выполняется проверка обновлений:

«Использовать только Интернет» –обновление будет загружено непосредственно с серверов PRO32.

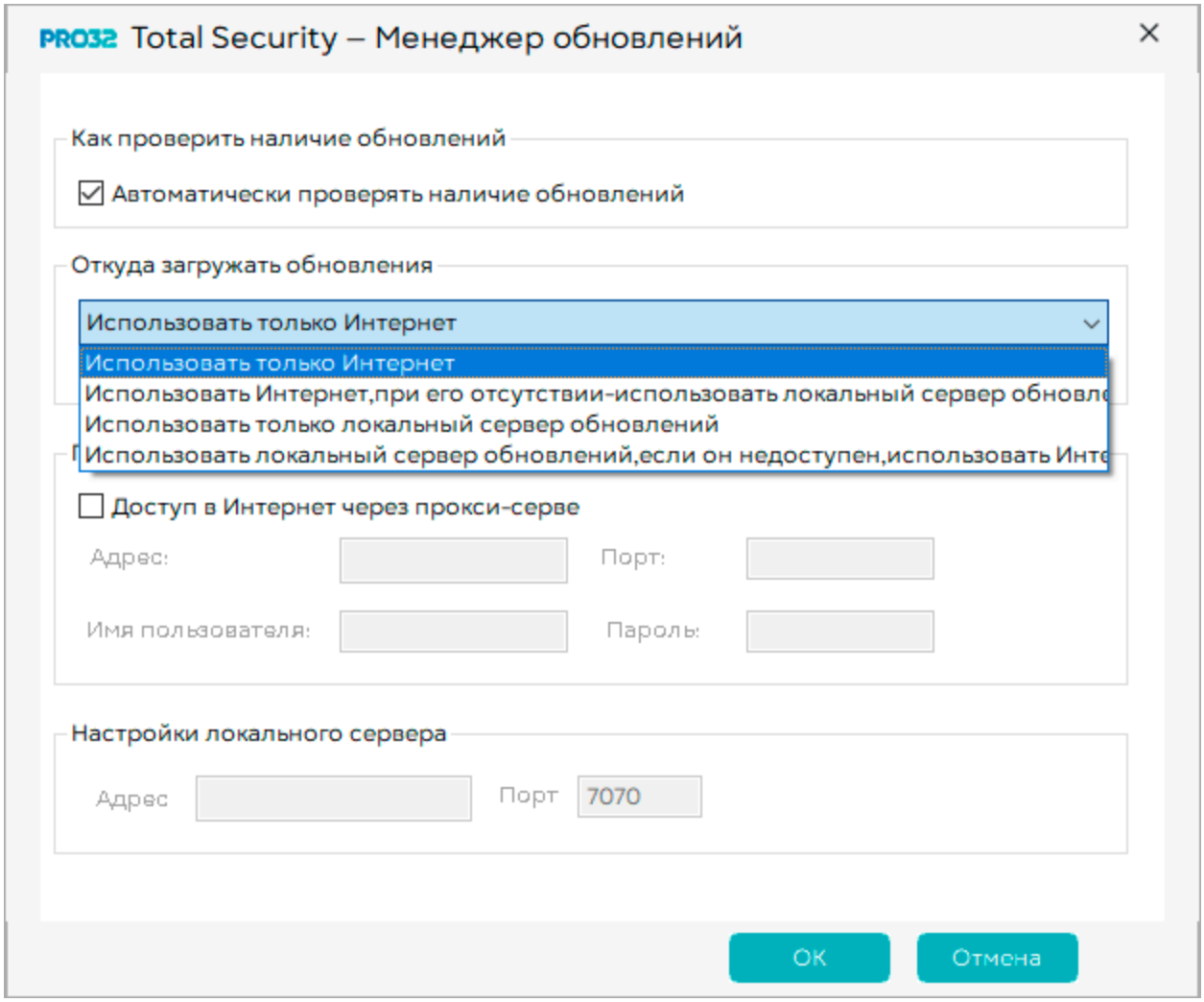
«Использовать Интернет, при отсутствии подключения использовать файлы с локального сервера обновлений» – файлы обновлений проверяются непосредственно на веб-сайте, если не удается подключиться к веб-сайту, система проверяет наличие обновлений на указанном локальном сервере обновлений. Можно задать адрес локального сервера обновления и порт в указанном ниже поле.

«Использовать только локальный сервер обновлений» – обновление будет взято с указанного локального сервера обновлений. Системы, не имеющие прямого подключения к Интернету, могут получать обновления с локального сервера обновлений.

«Использовать локальный сервер обновлений, если он недоступен – использовать Интернет» – локальный сервер проверяется на наличие последних обновлений. Если невозможно подключиться к локальному серверу обновлений, проверяется наличие обновлений на сервере PRO32.

5. Если ваше подключение к Интернету выполняется через прокси-сервер, установите флажок **«Доступ в Интернет через прокси-сервер»** и введите данные прокси-сервера в соответствующие поля.

6. Если требуется указать локальный сервер обновлений, укажите адрес локального сервера и номер порта в соответствующем поле.



7. Нажмите **«ОК»** для закрытия диалогового окна **«Режим обновлений»**

8. Убедитесь, что вы подключены к Интернету, и нажмите «Обновить сейчас» Продукт подключится к веб-сайту PRO32 и загрузит обновления. Будет показано сообщение со статусом обновления.

Для обновления вашего продукта у него должна быть действующая лицензия. Если срок действия лицензии истек, выводится предупреждение.

9. После обновления продукта вам нужно будет закрыть все открытые приложения и перезагрузить компьютер.

13.3. Отключение автоматических обновлений

Для обеспечения максимальной защиты рекомендуется настроить PRO32 Total Security на автоматическую загрузку и установку обновлений. Однако, если вы хотите обновлять свой продукт вручную, то функцию автоматического обновления можно отключить.

Для отключения автоматического обновления:

1. Откройте стартовый экран продукта , далее найдите **«Обновления»** в боковом меню, затем найдите кнопку **«Настройка обновлений»** .

2. Нажмите **«Режим обновлений»** .Откроется диалоговое окно **«Менеджер Обновлений».**

3. Установите флажок **«Автоматически проверять наличие обновлений».**

4. Нажмите **«ОК».**

Примечание: В случае отключения автоматического обновления вам необходимо будет проверять наличие обновлений вручную не реже двух раз в неделю, это позволит обеспечить актуальную защиту вашего компьютера.

14. Управление службой конфиденциальности

Всякий раз, когда вы просматриваете сайты в Интернете, компьютеры и веб-сайты, к которым вы подключаетесь, собирают информацию о вас. Часть этой информации собирается из форм, которые вы заполняете, и из ваших вариантов выбора. Другая информация может быть взята из вашего браузера, который предоставляет информацию о прошлой посещаемой веб-странице, и о типе компьютера, который вы используете.

При отправке информации через Интернет данные проходят через несколько компьютеров, прежде чем достигнут конечной точки. Во время передачи возможен перехват этой информации третьими лицами. Таким образом, злоумышленники могут собирать личные данные без вашего ведома.

Служба конфиденциальности помогает защитить вашу конфиденциальность за счет контроля информации, которую ваш браузер отправляет на веб-сайты. Служба также предотвращает доступ к несанкционированным веб-сайтам. Она позволяет создать список информации, которую вы хотите сохранить в тайне.

Вы можете предпринять одно из следующих действий:

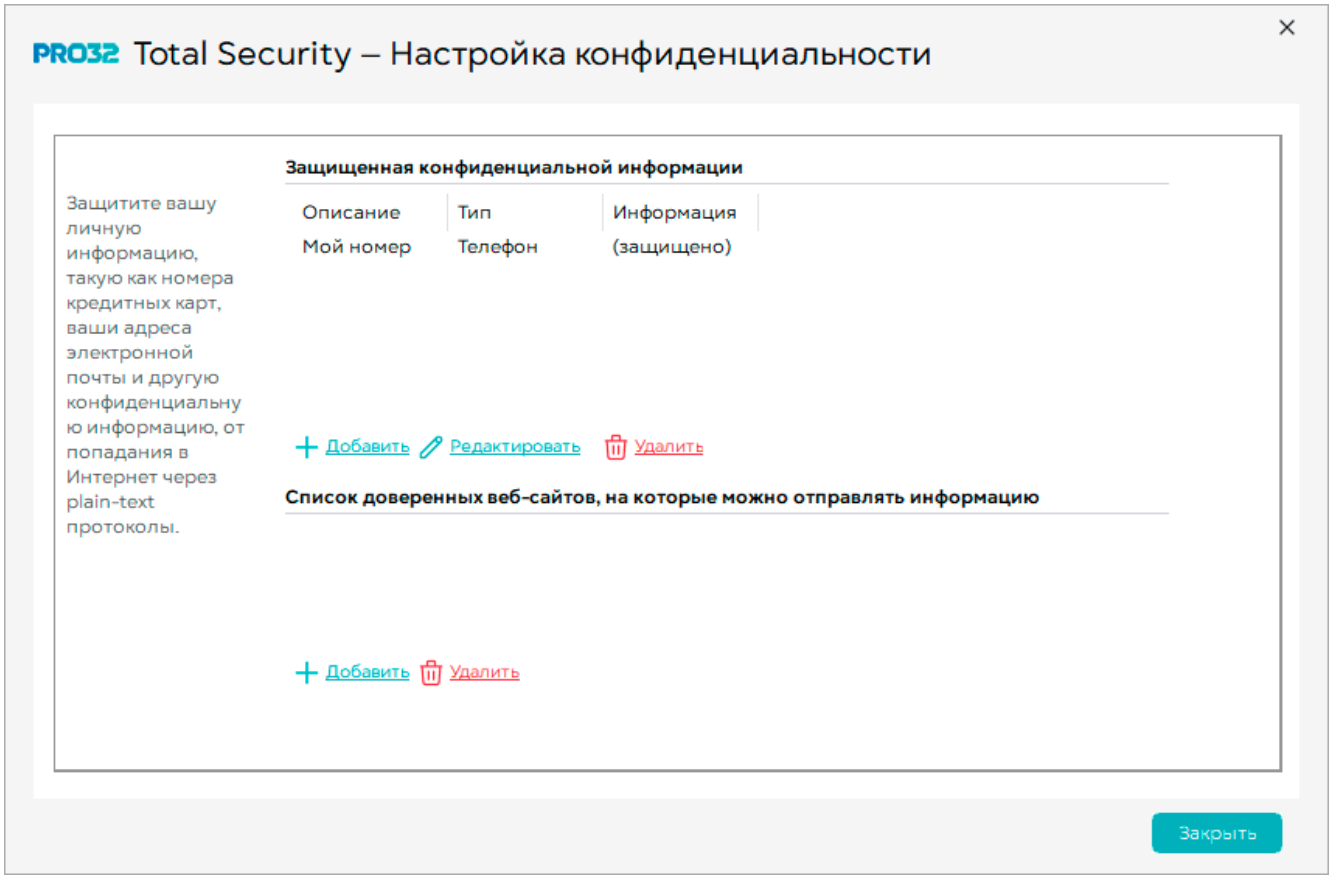
- Защитить конфиденциальную информацию
- Настроить список доверенных сайтов, которым будет доступна защищённая информация

Для настройки информации о конфиденциальности:

1. Откройте стартовый экран продукта , далее найдите **«Обновления»** в боковом меню.

3. Откроется диалоговое окно **«Настройка конфиденциальности».**

4. Доступны следующие действия:



Добавление информации о конфиденциальности

1. Нажмите кнопку «Добавить» + . Откроется диалоговое окно **«Конфиденциальная информация».**

2. Выберите категорию информации, которую необходимо защитить, в раскрывающемся списке Тип информации.

3. Введите Заголовок для информации. Это поможет запомнить информацию.

4Введите информацию, которую вы хотите защитить, в отведенном для этого поле.

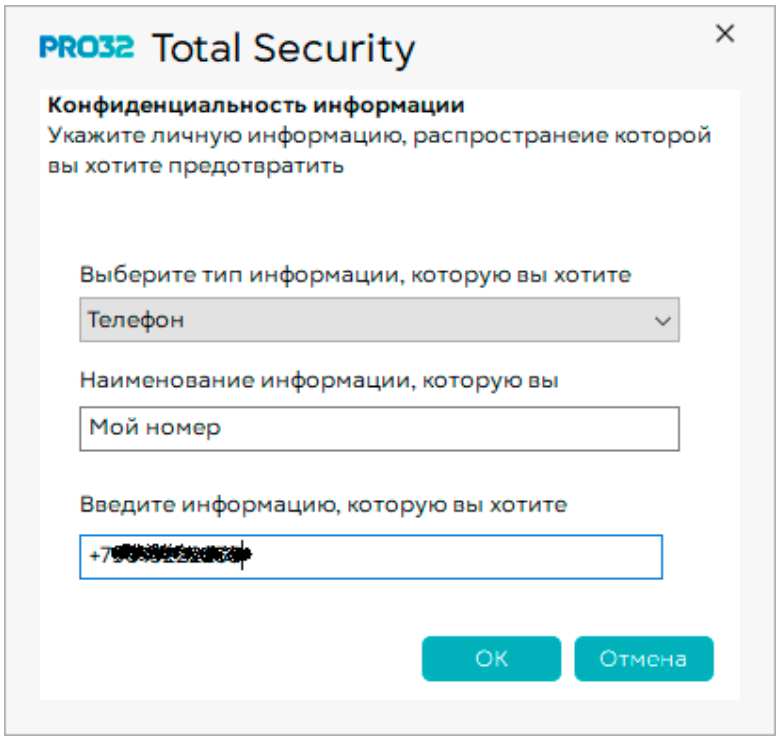
5. Нажмите **«ОК»,** чтобы сохранить информацию и вернуться в диалоговое окно «Настройка конфиденциальности». Информация будет добавлена в список Защищаемой конфиденциальной информации.

Редактирование информации о конфиденциальности

1. Нажмите кнопку «Редактировать» . Откроется диалоговое окно **«Конфиденциальная информация».**

2. Отредактируйте данные.

5. Нажмите **«ОК»,** чтобы сохранить информацию и вернуться в диалоговое окно «Настройка конфиденциальности». Информация будет добавлена в список Защищаемой конфиденциальной информации



Удаление информации о конфиденциальности

1. Откройте стартовый экран продукта, далее найдите **«Обновления»** в боковом меню.

2. Откроется диалоговое окно **«Настройка конфиденциальности».**

3. Выберите ту запись конфиденциальных данных, которую вы хотите удалить, затем нажмите кнопку «Удалить» .

14.1 Управление доверенными сайтами

PRO32 Total Security позволяет указывать надежные веб-сайты. Конфиденциальная информация, отправляемая на эти веб-сайты, не будет блокироваться функцией контроля конфиденциальности.

1. Откройте стартовый экран продукта, далее найдите **«Обновления»** в боковом меню.

2. Откроется диалоговое окно **«Настройка конфиденциальности».**

3. Нажмите кнопку Добавить +, чтобы указать надежные веб-сайты. Модуль не будет блокировать отправку информации о конфиденциальности на эти надежные веб-сайты.

4. Если вы хотите удалить веб-сайт из списка исключений, выберите веб-сайт и нажмите кнопку **«Удалить»**

15. Отчёты

PRO32 Total Security позволяет включать и отключать ведение журнала действий по защите от вредоносного ПО. Записи в журнале создаются при обнаружении вируса или другой вредоносной программы. В записях журнала вирусов также указывается время обнаружения вируса, тип сканирования, в ходе которого был обнаружен вирус, местонахождение вируса, имя файла, содержащего вирус, описание проблемы, статус файла и предпринятое действие.

Включение журнала Антивируса

1. Откройте стартовый экран продукта, затем **«Настройки защиты»** > , далее **«Настройки»** > модуля **«Антивирус и антишпион»** .
2. Откроется диалоговое окно настроек антивируса.
3. Нажмите вкладку «Прочее».

Вкладка содержит следующие параметры:

Предупреждать об истечении срока действия базы данных с информацией о вирусах.

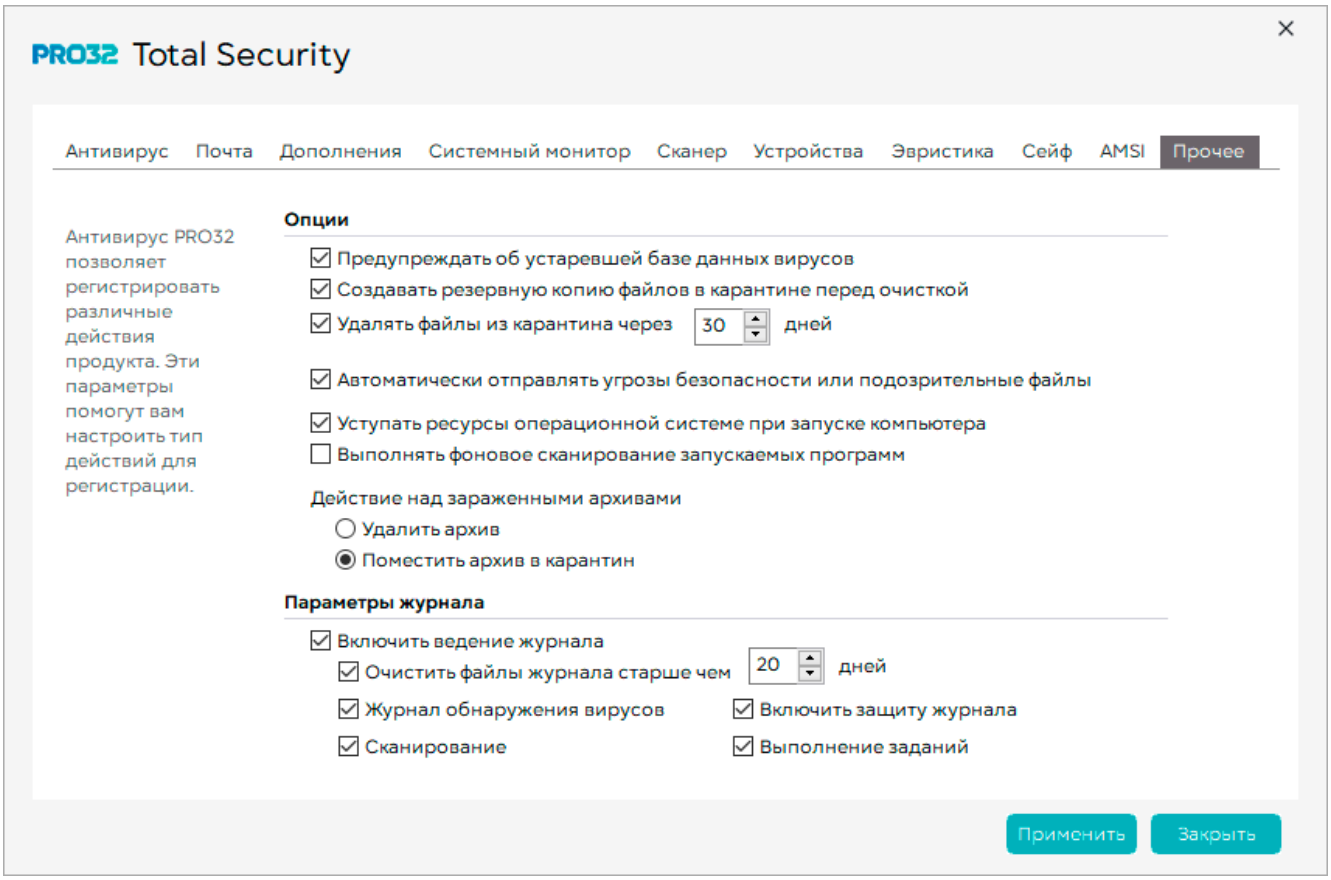
Отображает предупреждение, если определение вируса не обновлялось более 5 дней.

Создавать резервную копию файла в карантине перед очисткой

Создает копию карантинного файла в той же папке при выборе варианта очистки

Удалять файлы из карантина через «x» дней

Автоматически удаляет файлы, находящиеся в папке карантина, по истечении указанных «x» дней.



Включить контекстное меню в строке состояния

Отображает PRO32 Total Security в контекстном меню, вызываемом нажатием правой кнопкой мыши на значке PRO32 в области уведомлений.

Выполнять автоматические действия с зараженными архивами

Удалить архивы: если архив содержит один или несколько зараженных файлов, то он удаляется. Поместить архивы в карантин: если архив содержит один или несколько зараженных файлов, то он помещается в карантин

Автоматически отправлять угрозы безопасности или подозрительные файлы

Автоматически отправляет любые вредоносные файлы, на сервера PRO32 для их анализа. Выбор этого параметра позволяет вашему продукту участвовать в таких отправках.

Журнал обнаружения вирусов

Сохраняет сведения о вирусах, обнаруженных с помощью автоматического сканирования, сканера электронной почты, ручного сканирования, блокировки скриптов и блокировки червей, в отдельный файл

Удалять файлы журнала

Удаляет содержимое журнала, если он находился на вашем компьютере в течение старше «x» дней периода, превышающего 'x' дней.

Сканирование

Сохраняет сводку о результатах каждого сканирования, например, общее количество просканированных файлов, общее количество зараженных файлов и т.д., в отдельный файл.

Защита журнала

Записывает в журнал подробности, например, когда Антивирус, системный монитор или защита электронной почты Вкл./Выкл. отключается или включается.

Завершенные задачи

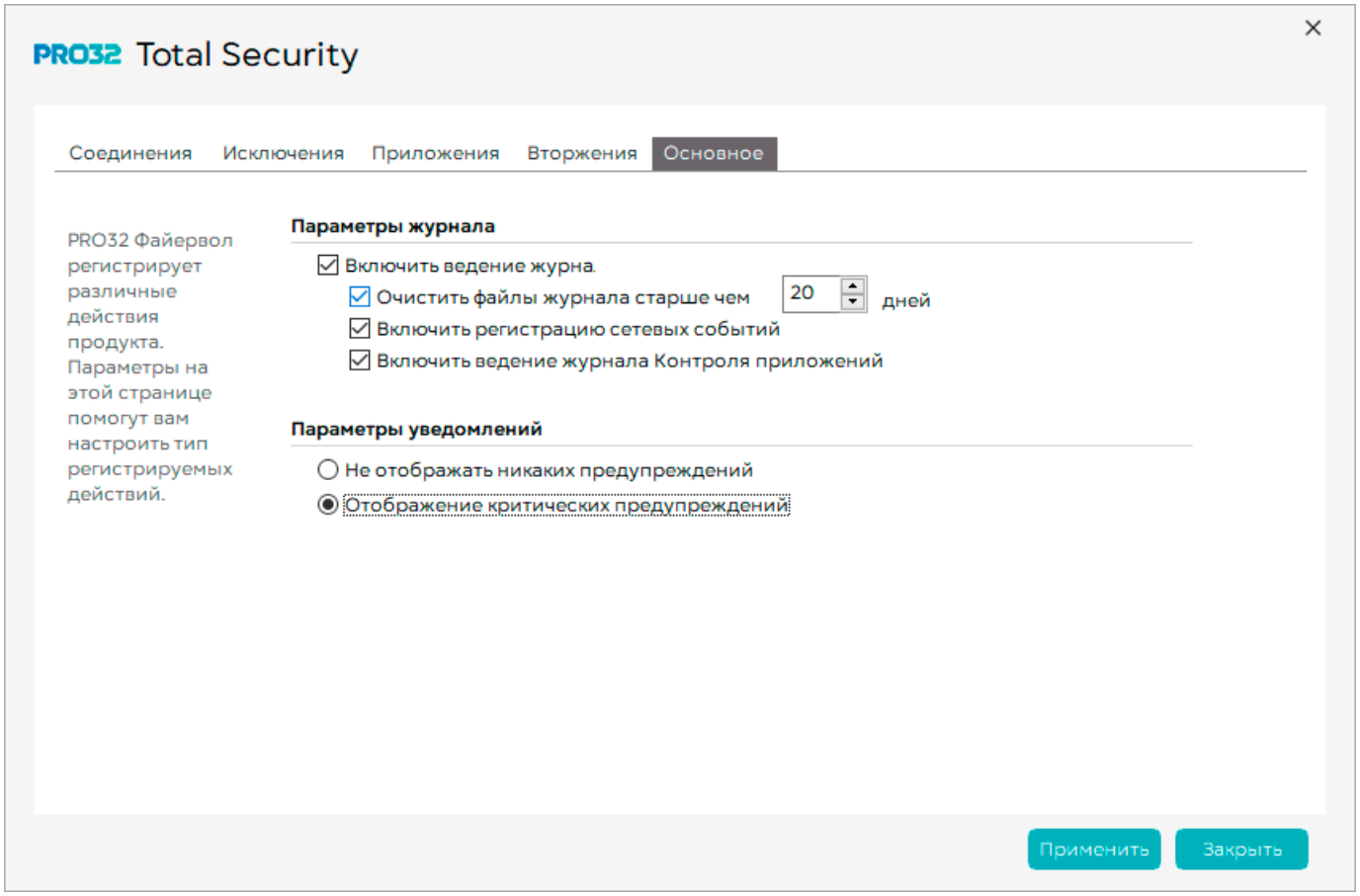
Сохраняет сведения о завершенных задачах сканирования в файл.

4. Нажмите кнопку **«Применить»** для сохранения настроек.

Включение журнала Файерволла

1. Откройте стартовый экран продукта, затем **«Настройки защиты»** > , далее **«Настройки»** > модуля **«Файерволл»** .
2. Откроется диалоговое окно настроек Файерволла. Откройте вкладку **«Основное».**
3. Параметры описаны в следующей таблице:

Параметр	Описание
Включить ведение журнала	Выберите эту опцию, если хотите, чтобы брандмауэр PRO32 регистрировал действия в журнале
Очистить файлы журнала старше «x» дней	Удаляет содержимое журнала возрастом более «x» дней
Включить регистрацию сетевых событий	Регистрирует сведения о трафике, заблокированном с применением правил брандмауэра.
Включить ведение журнала доступа к приложению	Регистрирует сведения о трафике, заблокированном с применением контроля доступа к приложениям.



4. Выбрать «**Параметры уведомлений»**. Параметры описаны в следующей таблице:

Параметр	Описание
Не отображать оповещения	Оповещения брандмауэра PRO32 отображаться не будут
Отображать оповещения	Отображает оповещение в случае блокировки трафика

15.1. Просмотр журналов

PRO32 Total Security хранит записи обо всех действиях, предпринятых в отношении различных служб защиты, входящих в его состав, а также об отслеживаемых действиях. Он регистрирует все обнаруженные вирусы, системные изменения, входящие и исходящие интернет-соединения, заблокированные соединения и действия по защите конфиденциальности. Вы можете просматривать эту информацию.

Средство просмотра журнала отображает журнал действий вашего продукта. Есть три категории журналов: защита от вредоносных программ, брандмауэр и конфиденциальность. Используя информацию в средстве просмотра журналов, вы можете просмотреть подробную информацию, записанную в каждом журнале, выбрав категорию журнала в левом столбце для отображения подробных сведений на правой панели.

1. Откройте стартовый экран продукта, далее найдите **«Отчёты»** в боковом меню.

2. Нажмите на **«События безопасности»** .

3. Откроется окно средства просмотра журнала.

4. Выберите модуль на левой панели.

5. Нажмите значок , чтобы развернуть модуль для просмотра параметров журнала.

6. Нажмите параметр журнала, чтобы отобразить соответствующие сведения на правой панели.

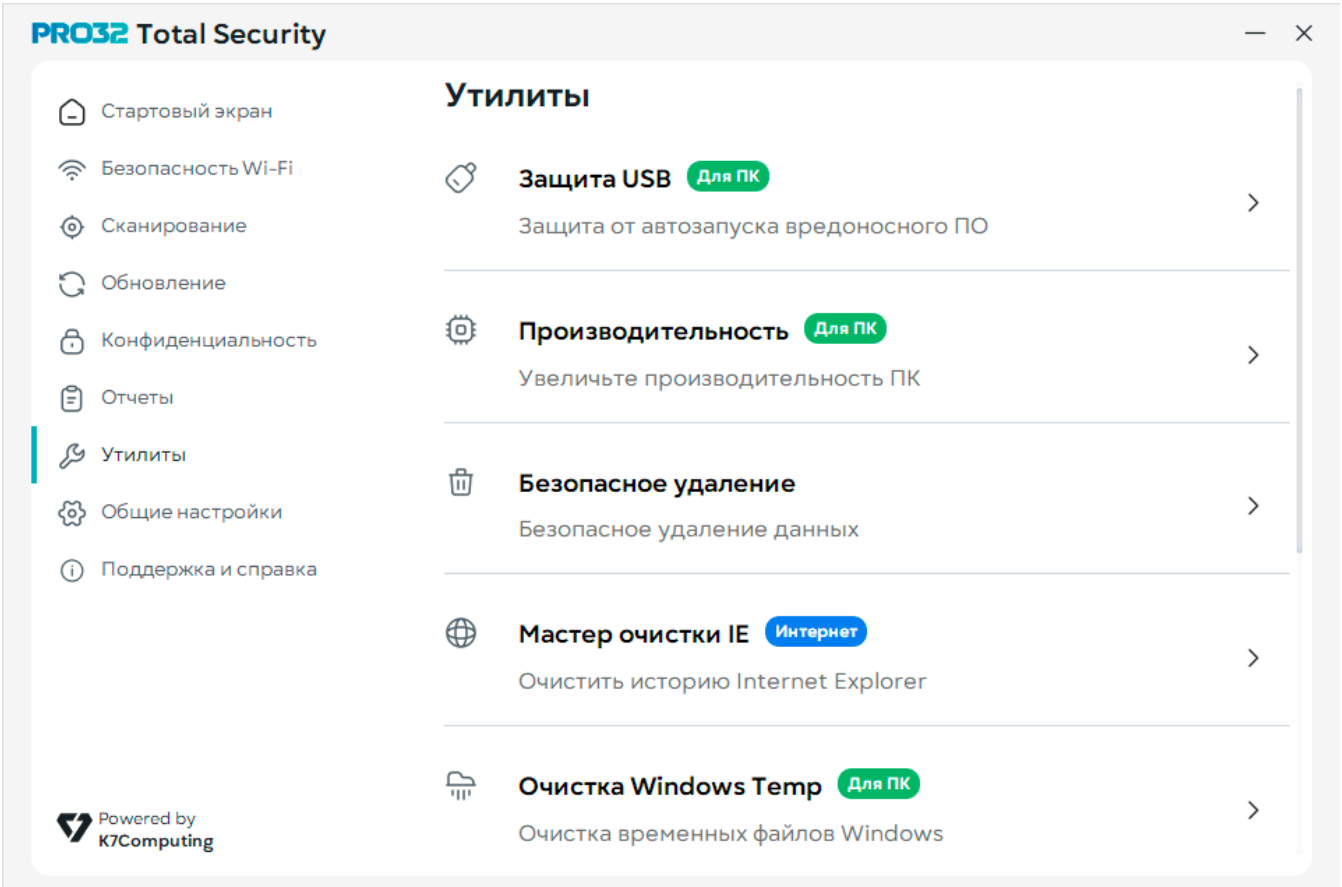
7. В меню средства просмотра журнала доступны следующие параметры:

Параметр	Описание
Сохранить	Сохраняет данные журнала в текстовый файл для дальнейшего использования. Введите имя и выберите путь для сохранения файла.
Обновить	Обновляет средство просмотра журнала, загружая последние зарегистрированные данные
Очистить	Очищает содержимое файла журнала
Справка	Открывает справку

8. Нажмите кнопку **«Закрыть»**, для закрытия средства просмотра журнала.

16. Утилиты

В этом разделе представлено множество полезных инструментов, которые помогут вам поддерживать и улучшать производительность системы, а также обеспечить ее безопасность. Этот раздел постоянно обновляется, чтобы вам всегда были доступны самые полезные инструменты.



«Вакцинация USB-устройств» – эта функция обеспечивает, что после вакцинации USB-накопителя он не сможет автоматически заражать компьютеры с использованием механизма автоматического выполнения.

«Виртуальная клавиатура» – программная клавиатура, отображаемая на экране для ввода данных с помощью мыши. Позволяет предотвратить кражу данных кейлоггерами.

«Точная настройка компьютера» – настраивайте параметры своего компьютера для повышения производительности. Для вступления в силу некоторых изменений может потребоваться перезагрузка. Вы также можете в любое время восстановить исходные настройки.

«Удаление журнала действий» – Windows сохраняет информацию о ваших недавно открытых документах и сведения о других действиях. Удаление этой информации не позволит другим пользователям просматривать вашу активность на компьютере.

«Windows Temp Cleaner» – приложения Windows часто создают временные файлы. Со временем они накапливаются и занимают много места на диске. Удаление этих нежелательных файлов освободит место на диске.

«Оптимизация диска» – эта функция переупорядочивает файлы, хранящиеся на жестком диске, чтобы увеличить скорость доступа.

«Средство очистки журнала IE» - Internet Explorer сохраняет данные о ранее посещенных URL-адресах на вашем компьютере. Удаление этой информации не позволит другим пользователям просматривать посещенные URL-адреса.

«Средство очистки временных файлов Интернета» - Internet Explorer сохраняет копии веб-контента на локальном диске. В результате на жестком диске накапливаются большие объемы данных. Удаление этих данных освободит место на жестком диске.

«Безопасное удаление» – функция безопасного удаления позволяет безопасно удалять файлы или папки и предотвращает просмотр или восстановление удаленных файлов другими пользователями.

Для использования инструментов:

1. Откройте стартовый экран продукта , далее найдите **«Утилиты»** в боковом меню.

2. Выберите нужный инструмент и нажмите кнопку « › ».

3. Следуйте указаниям на экране.

17. Общие настройки (Импорт\Экспорт настроек)

PRO32 Total Security помогает защитить ваш компьютер от новых возникающих угроз, включая сетевые вирусы, нежелательная электронная почта, неприемлемый контент и шпионское ПО, которые способны поставить под угрозу вашу конфиденциальность. Это позволяет вам полностью контролировать обмен данными как внутри вашего компьютера, так и с внешними получателями.

PRO32 Total Security использует заводские настройки по умолчанию во время установки, и для обеспечения безопасности своей системы вам не нужно совершать никаких лишних действий. Однако PRO32 Total Security позволяет настраивать параметры брандмауэра, расписания резервного копирования, а также параметры сканирования или защиты.

Вкладка Настройки позволяет настраивать различные параметры PRO32 Total Security. Внесенные в настройки изменения можно сохранить и при необходимости восстановить позже.

Для резервного копирования существующих настроек PRO32 Total Security:

1. Откройте стартовый экран продукта, далее найдите **«Общие настройки»** в боковом меню.

2. Нажмите кнопку «Настроить резервное копирование».
3. Нажмите **«Резервное копирование существующих настроек».** Откроется диалоговое окно **«Выберите или введите имя файла для резервного копирования».**

4. Укажите папку, в которой вы хотите сохранить файл, и введите имя файла. Настройки сохраняются в файл.dat.

Для восстановления сохраненных настроек PRO32 Total Security:

1. Откройте стартовый экран продукта, далее найдите **«Общие настройки»** в боковом меню.
2. Нажмите **«Восстановить из резервной копии».** Откроется диалоговое окно «Выберите или введите имя файла, используемого для восстановления».

4. Укажите файл (.dat) с требуемыми настройками и нажмите Открыть.

Вы можете восстановить настройки PRO32 Total Security до исходных настроек, заданных при установке.

Для сброса настроек по умолчанию.

1. Откройте стартовый экран продукта, далее найдите **«Общие настройки»** в боковом меню.
2. Нажмите «Восстановить заводские настройки». Система предупредит о сбросе существующих настроек и попросит подтвердить действие.

4. Если выбрать **«Да»,** будет выполнен возврат к заводским настройкам по умолчанию.

Примечание: чтобы изменения вступили в силу, потребуется перезагрузка компьютера.

Установка пароля

Настройки PRO32 Total Security можно защитить с помощью пароля. Это предотвратит несанкционированный доступ к продукту.

Чтобы установить пароль для защиты настроек:

1. Откройте стартовый экран продукта, далее найдите **«Общие настройки»** в боковом меню.
2. Выберите вариант **«Требуется пароль для изменения настроек и отключения защиты».**

4. Выберите **«Нажмите здесь для изменения или установки пароля, чтобы задать выбранный пароль».**

Настройка оповещений

PRO32 Total Security автоматически выдает предупреждение в случае обнаружения угрозы или вирусной атаки. Вы также будете получать оповещения, когда на вашем компьютере происходят изменения или когда будут завершены обновления. Предупреждения отображаются во всплывающих окнах и содержат текстовую область, в которой отображается сообщение.

Вы можете настроить внешний вид всплывающего окна, а также способ отображения предупреждений.

Для настройки предупреждений:

1. Откройте стартовый экран продукта, далее найдите **«Общие настройки»** в боковом меню.
2. Установите флажки для необходимых параметров. Параметры описаны в следующей таблице.

Параметр	Описание
Отображать заставку при запуске	Отображает заставку при запуске PRO32 Total Security. Этот параметр выбран по умолчанию.
Отображать некритические сообщения	Отображает все предупреждения, в том числе критические и некритические.

3. Нажмите кнопку Закрыть для сохранения настроек.

4. После настройки параметров предупреждений вы можете выполнить одно из следующих действий:

- Резервное копирование настроек продукта
- Восстановление настроек продукта из резервной копии
- Загрузка настроек, заданных при установке