ENDPOINT SECURITY

для macOS

Руководство пользователя

(для продукта, начиная с версии 6.0)

Щелкните здесь, чтобы загрузить последнюю версию этого документа.

Служба поддержки клиентов: www.eset.com/support

Версия 24. 4. 2017

Содержание

1. ESET Endpoint Security....4
1.1 Новые возможности версии 6....4
1.2 Требования к системе....4
2. Пользователи, подключающиеся через ESET Remote Administrator....4
2.1 ESET Remote Administrator Server....5
2.2 Веб-консоль....5
2.3 Прокси-сервер....6
2.4 Агент....6
2.5 RD Sensor....6
3. Установка....6
3.1 Обычная установка....7
3.2 Выборочная установка....7
3.3 Удаленная установка....8
3.3.1 Создание пакета удаленной установки....8
3.3.2 Удаленная установка на целевые компьютеры....9
3.3.3 Удаленное удаление....9
3.3.4 Удаленное обновление....9
4. Активация программы....9
5. Удаление....10
6. Краткий обзор интерфейса программы....10
6.1 Сочетания клавиш....11
6.2 Проверка работоспособности системы....11
6.3 Устранение неполадок программы....11
7. Защита компьютера....11
7.1 Защита от вирусов и шпионских программ....11
7.1.1 Общие параметры....12
7.1.1.1 Исключения....12
7.1.2 Защита при запуске....12
7.1.3 Защита файловой системы в режиме реального времени....13
7.1.3.1 Расширенные параметры....13
7.1.3.2 Изменение параметров защиты в режиме реального времени....13
7.1.3.3 Проверка защиты в режиме реального времени....14
7.1.3.4 Устранение неполадок с неработающим модулем защиты в режиме реального времени....14
7.1.4 Сканирование компьютера по требованию....14
7.1.4.1 Тип сканирования....15
7.1.4.1.1 Сканирование Smart....15
7.1.4.1.2 Выборочное сканирование....15
7.1.4.2 Объекты сканирования....15
7.1.4.3 Профили сканирования....15
7.1.5 Настройка параметров модуля ThreatSense....16
7.1.5.1 Объекты....16
7.1.5.2 Параметры....17
7.1.5.3 Очистка....17
7.1.5.4 Исключения....17
7.1.5.5 Ограничения....18
7.1.5.6 Другие настройки....18
7.1.6 Действия при обнаружении заражения....18
7.2 Защита доступа в Интернет и электронной почты....19
7.2.1 Защита доступа в Интернет....19
7.2.1.1 Порты....19
7.2.1.2 Списки URL-адресов....19
7.2.2 Защита электронной почты....19
7.2.2.1 Проверка протокола POP3....20
7.2.2.2 Проверка протокола IMAP....20
7.3 Защита от фишинга....20
8. Файервол....21
8.1 Режимы фильтрации....21
8.2 Правила файервола....21
8.2.1 Создание правил....22
8.3 Зоны файервола....22
8.4 Профили файервола....22
8.5 Журналы файервола....22
9. Контроль устройств....23
9.1 Редактор правил....23
10. Контроль доступа в Интернет....24
11. Служебные программы....25
11.1 Файлы журналов....25
11.1.1 Обслуживание журналов....26
11.1.2 Фильтрация журнала....26
11.2 Планировщик....27
11.2.1 Создание задач....27
11.2.2 Создание пользовательской задачи....28
11.3 Live Grid....28
11.3.1 Подозрительные файлы....29
11.4 Карантин....29
11.4.1 Помещение файлов на карантин....29
11.4.2 Восстановление файла из карантина....30
11.4.3 Отправка файла из карантина....30
11.5 Права....30
11.6 Режим презентации....30
11.7 Запущенные процессы....31
12. Интерфейс....32
12.1 Предупреждения и уведомления....32
12.1.1 Отображение предупреждений....32
12.1.2 Состояния защиты....33
12.2 Контекстное меню....33
13. Обновление....33
13.1 Настройка обновлений....33
13.1.1 Расширенные параметры....34
13.2 Создание задач обновления....35
13.3 Обновление до новой сборки....35
13.4 Обновления системы....35
14. Разное....36
14.1 Импорт и экспорт параметров....36
14.2 Настройка прокси-сервера....36
14.3 Общий локальный кэш....36

1. ESET Endpoint Security

Программа ESET Endpoint Security 6 представляет собой новый подход к созданию действительно комплексной системы безопасности компьютера. Актуальная версия модуля сканирования ThreatSense®в сочетании с нашим персональным файерволом обеспечивает скорость и точность, необходимые для обеспечения безопасности компьютера. Таким образом, продукт представляет собой интеллектуальную систему непрерывной защиты от атак и вредоносных программ, которые могут угрожать безопасности компьютера.

Программа ESET Endpoint Security 6 — это комплексное решение для обеспечения безопасности, являющееся результатом долгих усилий, направленных на достижение оптимального сочетания максимальной степени защиты с минимальным влиянием на производительность компьютера. Современные технологии, основанные на применении искусственного интеллекта, способны профилактически защищать ПК от вирусов, шпионских, троянских и рекламных программ, червей, руткитов и других атак из Интернета без влияния на производительность компьютера и перерывов в работе.

Эта программа предназначена в первую очередь для использования на рабочих станциях в средах небольших и крупных предприятий. Его можно использовать с ESET Remote Administrator 6, что позволяет с легкостью управлять любым количеством клиентских рабочих станций, применять политики и правила, отслеживать обнаруживаемые угрозы и удаленно настраивать систему с любого подключенного к сети компьютера.

1.1 Новые возможности версии 6

Графический интерфейс программы ESET Endpoint Security полностью изменен: внешний вид стал лучше, а работа с приложением — более интуитивно понятной. Ниже приведены некоторые улучшения в шестой версии приложения.

- **Файервол**: теперь можно создавать правила файервола непосредственно на основе журнала или уведомления IDS (Intrusion detection system) и назначать профили для сетевых интерфейсов.
- **Контроль доступа в Интернет**: блокирует веб-страницы, которые могут содержать потенциально нежелательные материалы.
- **Защита доступа в Интернет**: отслеживает обмен данными между веб-браузерами и удаленными серверами.
- **Защита электронной почты**: обеспечивает контроль сообщений, полученных по протоколам POP3 и IMAP.
- **Защита от фишинга**: защищает от попыток получить пароли и другую конфиденциальную информацию, запрещая доступ к вредоносным веб-сайтам, которые принимают вид нормальных веб-сайтов.
- **Контроль устройств**: с помощью этой функции можно сканировать, блокировать и/или изменять расширенные фильтры и/или разрешения, а также указывать, может ли пользователь получать доступ к внешним устройствам и работать с ними. Эта функция доступна в версии программы 6.1 и более поздних версиях.
- **Режим презентации**: позволяет ESET Endpoint Security работать в фоновом режиме и блокирует все всплывающие окна и запланированные задачи.
- **Общий локальный кэш**: повышает скорость сканирования в виртуализированных средах.

1.2 Требования к системе

Для оптимальной работы ESET Endpoint Security система должна отвечать указанным ниже требованиям к оборудованию и программному обеспечению.

	Требования к системе
Архитектура процессора	Intel, 32- или 64-разрядная
Операционная система	macOS 10.9 и более поздние версии
Объем памяти	300 МБ
Объем свободного места на диске	200 МБ

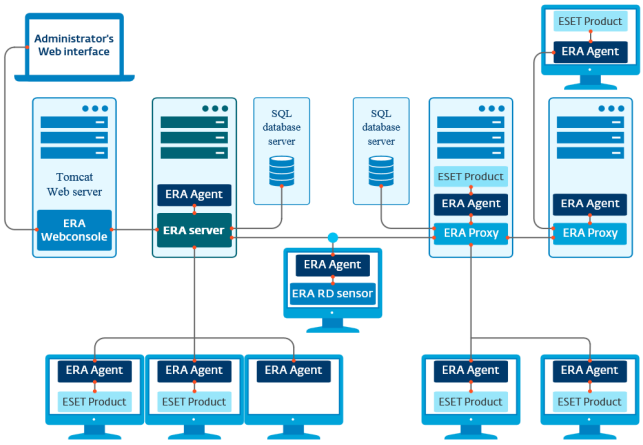
2. Пользователи, подключающиеся через ESET Remote Administrator

ESET Remote Administrator (ERA) 6 — это приложение, позволяющее осуществлять централизованное управление продуктами ESET, установленными в сетевой среде. Система управления задачами ESET Remote Administrator позволяет установить решения ESET для обеспечения безопасности на удаленные компьютеры и быстро реагировать на новые проблемы и угрозы. Решение ESET Remote Administrator не предоставляет защиту от

вредоносного кода. Для защиты на каждом клиенте должно использоваться соответствующее решение ESET.

В решениях ESET для обеспечения безопасности предусмотрена поддержка сетей, использующих несколько платформ различных типов. В сети могут одновременно присутствовать операционные системы Microsoft, Linux и Mac OS, а также системы, работающие на мобильных устройствах (мобильных телефонах и планшетах).

На рисунке ниже представлен пример архитектуры сети, защищенной решениями ESET для обеспечения безопасности. Этими решениями управляет приложение ERA.



ПРИМЕЧАНИЕ. Дополнительные сведения см. в ESET Remote Administratorдокументации в Интернете.

2.1 ESET Remote Administrator Server

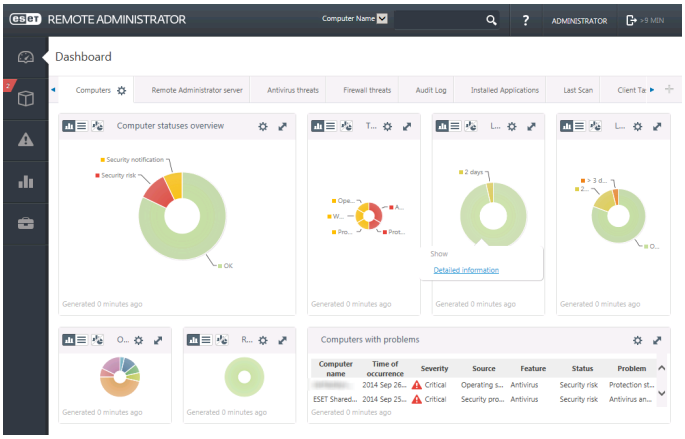
Сервер ESET Remote Administrator Server является управляющим компонентом продукта ESET Remote Administrator. Он обрабатывает все данные, получаемые от клиентов, которые подключаются к серверу посредством агента ERA 6. Агент ERA упрощает обмен данными между клиентом и сервером. Данные (журналы клиентов, файлы конфигурации и репликации агентов и т. д.) хранятся в базе данных, которую решение ERA использует для создания отчетов.

Для правильной обработки данных серверу ERA требуется стабильное соединение с сервером базы данных. Для оптимальной производительности рекомендуется установить сервер ERA и базу данных на разные серверы. Компьютер, на котором установлен сервер ERA, должен быть настроен на прием всех запросов на подключение от агентов, прокси-сервера и компонента RD Sensor. Такие подключения проходят проверку с использованием сертификатов. После установки сервера ERA становится доступной веб-консоль ERA 5, позволяющая управлять конечными рабочими станциями, на которых установлены решения ESET.

2.2 Веб-консоль

Веб-консоль ERA — это приложение с веб-интерфейсом, которое отображает данные, полученные с сервера ERA 5, и позволяет управлять решениями безопасности ESET в сети. Доступ к веб-консоли осуществляется с помощью браузера. В ней отображаются общие сведения о состоянии клиентов в сети, и ее можно использовать для удаленного развертывания решений ESET на неуправляемых компьютерах. Если разрешить доступ к веб-серверу из Интернета, решение ESET Remote Administrator можно будет использовать практически в любом месте и на любом устройстве.

Панель мониторинга веб-консоли



В верхней части консоли расположено средство **Быстрый поиск**. В раскрывающемся меню выберите пункт **Имя компьютера**, **Адрес IPv4/IPv6** или **Имя угрозы**, введите в текстовое поле поисковую фразу и щелкните значок лупы (или нажмите клавишу **ВВОД**), чтобы выполнить поиск. Вы будете перенаправлены в раздел «Группы», где будут показаны результаты поиска.

2.3 Прокси-сервер

Прокси-сервер ERA — это еще один компонент ESET Remote Administrator, который выполняет две функции. В сетях среднего размера и корпоративных сетях с большим количеством клиентов (например, 10 000 и больше) прокси-сервер ERA может использоваться для распределения нагрузки между несколькими прокси-серверами ERA, снижая таким образом нагрузку на главный сервер ERA [5]. Другим преимуществом прокси-сервера ERA является то, что его можно использовать для подключения к удаленном филиалу со слабой связью. Это означает, что установленные на всех клиентах агенты ERA подключаются не к главному серверу ERA, а к прокси-серверу ERA, который находится в локальной сети филиала. Таким образом освобождается канал связи с филиалом. Прокси-сервер ERA принимает подключения от всех локальных агентов ERA, получает от них данные и передает их на главный сервер ERA (или другой прокси-сервер ERA). Это позволяет включать в сеть больше клиентов без ухудшения ее производительности и обработки запросов к базе данных.

В зависимости от конфигурации сети прокси-сервер ERA может подключаться к главному серверу ERA через другой прокси-сервер.

Чтобы прокси-сервер ERA работал надлежащим образом, на главном компьютере, на котором этот сервер установлен, нужно установить агент ESET, а сам компьютер следует подключить к верхнему уровню сети (серверу ERA или прокси-серверу ERA верхнего уровня, если такой имеется).

2.4 Агент

Агент ERA является важным компонентом программы ESET Remote Administrator. Решения по обеспечению безопасности ESET, работающие на клиентских компьютерах (например, ESET Endpoint Security), обмениваются данными с сервером ERA через агенты. Это позволяет централизованно управлять решениями безопасности ESET, установленными на удаленных клиентах. Агент собирает информацию на клиенте и отправляет ее на сервер. Когда сервер отправляет задачу клиенту, ее вначале получает агент, который затем направляет ее клиенту. Передача данных по сети происходит между агентом и верхним уровнем сети ERA — сервером и прокси-сервером.

Для связи с сервером агент ESET использует один из трех методов, указанных ниже:

1. Агент клиента напрямую связывается с сервером.
2. Агент клиента связывается с сервером через прокси-сервер.
3. Агент клиента связывается с сервером через несколько прокси-серверов.

Агент ESET обменивается данными с установленными на клиенте решениями ESET, собирает информацию о программах, используемых на таком клиенте, и передает клиенту полученные от сервера сведения о конфигурации.

ПРИМЕЧАНИЕ: У прокси-сервера ESET есть собственный агент, отвечающий за обмен данными с клиентами, другими прокси-серверами и сервером.

2.5 RD Sensor

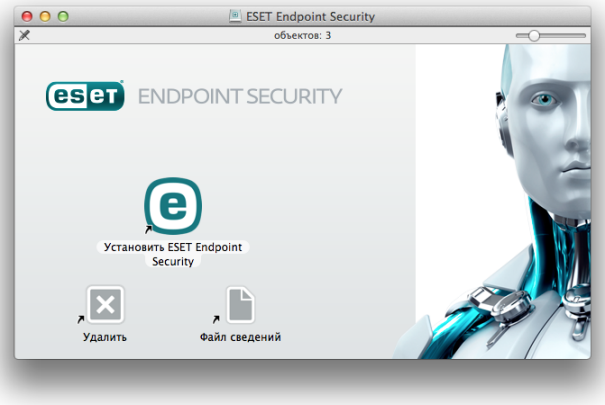
RD (Rogue Detection) Sensor — это входящий в состав ESET Remote Administrator инструмент поиска компьютеров в сети. Он позволяет быстро добавлять новые компьютеры в ESET Remote Administrator без необходимости искать и добавлять их вручную. Каждый обнаруженный в сети компьютер отображается в веб-консоли и добавляется в стандартную группу «Все», после чего с отдельными клиентскими компьютерами можно выполнять дополнительные действия.

Средство RD Sensor пассивно прослушивает сеть, обнаруживает находящиеся в ней компьютеры и направляет информацию о них серверу ERA. Затем сервер ERA проверяет, являются ли обнаруженные ПК неизвестными или уже находятся под его управлением.

3. Установка

Запустить установочный файл ESET Endpoint Security можно двумя способами:

- Если для установки используется установочный CD/DVD-диск, вставьте его в дисковод (CD/DVD-ROM) и дважды щелкните значок установки ESET Endpoint Security, чтобы запустить установщик.
- Если установка выполняется с помощью загруженного файла, дважды щелкните этот файл, чтобы запустить установщик.



Мастер установки поможет настроить основные параметры приложения. На начальной стадии установки установщик автоматически проверяет в Интернете наличие последней версии программы. При наличии более новой версии система, прежде чем продолжить процесс установки, предлагает загрузить эту версию.

После принятия лицензионного соглашения можно выбрать один из указанных ниже типов установки.

- Обычная установка 7
- Выборочная установка 7
- Удаленная установка 8

3.1 Обычная установка

В режиме обычной установки используются параметры, подходящие для большинства пользователей. Эти параметры обеспечивают максимальную защиту и высокую производительность системы. Обычная установка — это вариант по умолчанию. При отсутствии особых требований не следует выбирать другой способ.

ESET Live Grid
Благодаря системе своевременного обнаружения ESET Live Grid компания ESET постоянно получает своевременную информацию о новых заражениях и имеет возможность оперативно защищать пользователей. Эта система обеспечивает отправку новых угроз в лабораторию ESET по изучению угроз, где они анализируются, обрабатываются и добавляются в базу данных сигнатур вирусов. Для изменения параметров отправки подозрительных файлов нажмите кнопку **Настройка**. Дополнительные сведения см. в разделе Live Grid 28.

Потенциально нежелательные приложения
Последним действием при установке является настройка обнаружения **потенциально нежелательных приложений**. Такие программы могут не быть вредоносными, однако они часто негативно влияют на работу операционной системы. Они зачастую поставляются вместе с полезными приложениями, и их установку может быть трудно заметить во время установки всего пакета программ. Хотя при установке таких приложений обычно отображается уведомление, они вполне могут быть установлены без согласия пользователя.

После установки ESET Endpoint Security следует выполнить сканирование компьютера на наличие вредоносного кода. В главном окне программы выберите пункт **Сканирование компьютера**, а затем — **Сканирование Smart**. Дополнительные сведения о сканировании компьютера по требованию см. в разделе Сканирование компьютера по требованию 14.

3.2 Выборочная установка

Режим выборочной установки предназначен для опытных пользователей, которые хотят изменить дополнительные параметры в ходе установки.

Компоненты программы
Решение ESET Endpoint Security можно установить без некоторых основных компонентов (например, без защиты Интернета и электронной почты). Снимите флажки возле компонентов, которые не нужно устанавливать.

Прокси-сервер
Если вы используете прокси-сервер, его параметры можно указать, установив флажок **Я использую прокси-сервер**. Далее введите IP-адрес или URL-адрес прокси-сервера в поле **Адрес**. В поле «Порт» укажите порт, по которому прокси-сервер принимает запросы на соединение (3128 — это порт, используемый по умолчанию). Если на прокси-сервере требуется аутентификация, введите правильные **имя пользователя** и **пароль**, которые необходимы для доступа к прокси-серверу. Если прокси-сервер не используется, выберите вариант **Я не использую прокси-сервер**. Если вы не уверены в выборе, используйте текущие системные параметры, установив флажок **Системные параметры (рекомендуется)**.

Права
На следующем этапе можно определить пользователей или группы пользователей с правами, которые смогут изменять конфигурацию программы. Чтобы добавить пользователей в список **Пользователи с правами**, выберите их в списке в левой части окна и нажмите кнопку **Добавить**. Чтобы отобразить всех пользователей системы, установите флажок **Показывать всех пользователей**. Если список «Пользователи с правами» пуст, все пользователи смогут изменять конфигурацию программы.

ESET Live Grid
Благодаря системе своевременного обнаружения ESET Live Grid компания ESET постоянно получает своевременную информацию о новых заражениях и имеет возможность оперативно защищать пользователей. Эта система обеспечивает отправку новых угроз в лабораторию ESET по изучению угроз, где они анализируются, обрабатываются и добавляются в базу данных сигнатур вирусов. Для изменения параметров отправки подозрительных файлов нажмите кнопку **Настройка**.
Дополнительные сведения см. в разделе Live Grid 28.

Потенциально нежелательные приложения
На следующем этапе установки нужно настроить обнаружение **потенциально нежелательных приложений**. Такие программы могут не быть вредоносными, однако они часто негативно влияют на работу операционной системы. Они зачастую поставляются вместе с полезными приложениями, и их установку может быть трудно заметить во время установки всего пакета программ. Хотя при установке таких приложений обычно отображается уведомление, они вполне могут быть установлены без согласия пользователя.

Файервол
Выберите режим фильтрации для файервола. Дополнительные сведения см. в разделе Режимы фильтрации 21.

После установки ESET Endpoint Security следует выполнить сканирование компьютера на наличие вредоносного кода. В главном окне программы выберите пункт **Сканирование компьютера**, а затем — **Сканирование Smart**. Дополнительную информацию о сканировании компьютера по требованию см. в разделе Сканирование компьютера по требованию 14.

3.3 Удаленная установка

Вы можете создать пакет установки и установить его на целевых компьютерах с помощью ПО для работы с удаленными рабочими столами. Установленной программой ESET Endpoint Security можно управлять удаленно с помощью ESET Remote Administrator.

Удаленная установка состоит из двух этапов.
1. Создание пакета удаленной установки с помощью установщика ESET 8
2. Удаленная установка с помощью ПО для работы с удаленными рабочими столами 9

С помощью последней версии ESET Remote Administrator 6 также можно выполнять удаленную установку на клиентских компьютерах под управлением macOS. Подробные инструкции см. в этой статье базы знаний (статья доступна не на всех языках).

3.3.1 Создание пакета удаленной установки

Компоненты программы
Решение ESET Endpoint Security можно установить без некоторых основных компонентов (например, без защиты Интернета и электронной почты). Снимите флажки возле компонентов, которые не нужно устанавливать.

Прокси-сервер
Если вы используете прокси-сервер, его параметры можно указать, установив флажок **Я использую прокси-сервер**. Далее введите IP-адрес или URL-адрес прокси-сервера в поле **Адрес**. В поле «Порт» укажите порт, по которому прокси-сервер принимает запросы на соединение (3128 — это порт, используемый по умолчанию). Если на прокси-сервере требуется аутентификация, введите правильные **имя пользователя** и **пароль**, которые необходимы для доступа к прокси-серверу. Если прокси-сервер не используется, выберите вариант **Я не использую прокси-сервер**. Если вы не уверены в выборе, используйте текущие системные параметры, установив флажок **Системные параметры (рекомендуется)**.

Права
На следующем этапе можно определить пользователей или группы пользователей с правами, которые смогут изменять конфигурацию программы. Чтобы добавить пользователей в список **Пользователи с правами**, выберите их в списке в левой части окна и нажмите кнопку **Добавить**. Чтобы отобразить всех пользователей системы, установите флажок **Показывать всех пользователей**. Если список «Пользователи с

правами» пуст, все пользователи смогут изменять конфигурацию программы.

ESET Live Grid
Благодаря системе своевременного обнаружения ESET Live Grid компания ESET постоянно получает своевременную информацию о новых заражениях и имеет возможность оперативно защищать пользователей. Эта система обеспечивает отправку новых угроз в лабораторию ESET по изучению угроз, где они анализируются, обрабатываются и добавляются в базу данных сигнатур вирусов. Для изменения параметров отправки подозрительных файлов нажмите кнопку **Настройка**.
Дополнительные сведения см. в разделе Live Grid 28.

Потенциально нежелательные приложения
На следующем этапе установки нужно настроить обнаружение **потенциально нежелательных приложений**. Такие программы могут не быть вредоносными, однако они часто негативно влияют на работу операционной системы. Они зачастую поставляются вместе с полезными приложениями, и их установку может быть трудно заметить во время установки всего пакета программ. Хотя при установке таких приложений обычно отображается уведомление, они вполне могут быть установлены без согласия пользователя.

Файервол
Выберите режим фильтрации для персонального файервола. Дополнительные сведения см. в разделе Режимы фильтрации 21.

Файлы удаленной установки
На последнем этапе работы мастера установки выберите целевую папку для пакета установки (esets_remote_Install.pkg), сценария оболочки установки (esets_setup.sh) и сценария оболочки удаления (esets_remote_UnInstall.sh).

3.3.2 Удаленная установка на целевые компьютеры

На целевые компьютеры программу ESET Endpoint Security можно установить с помощью приложения Apple Remote Desktop или другого ПО, поддерживающего установку стандартных пакетов macOS (.pkg). Для установки программы скопируйте на целевые компьютеры файлы и запустите на них сценарии оболочки.

Чтобы установить ESET Endpoint Security с помощью Apple Remote Desktop, выполните следующие действия.

1. Щелкните значок **Копировать** в Apple Remote Desktop.
2. Нажмите кнопку **+**, перейдите к сценарию оболочки установки (esets_setup.sh) и выберите его.
3. Выберите в раскрывающемся меню **Поместить объекты в** расположение **/tmp** и щелкните **Копировать**.
4. Щелкните элемент **Установить**, чтобы отправить пакет на целевые компьютеры.

Подробные инструкции по администрированию клиентских компьютеров с помощью средства ESET Remote Administrator см. в интернет-документации ESET Remote Administrator.

3.3.3 Удаленное удаление

Чтобы удалить приложение ESET Endpoint Security с клиентских компьютеров, выполните описанные ниже действия.

1. Выполните в программе Apple Remote Desktop команду **Копировать объекты**, выберите сценарий оболочки удаления (*esets_remote_unInstall.sh*, создается вместе с установочным пакетом) и скопируйте его на целевые компьютеры в каталог /tmp (например, */tmp/esets_remote_uninstall.sh*).
2. В разделе **Запустить команду как** выберите элемент «Пользователь» и в поле **Пользователь** введите **root**.
3. Щелкните элемент **Отправить**. По завершении удаления в консоли отобразится журнал.

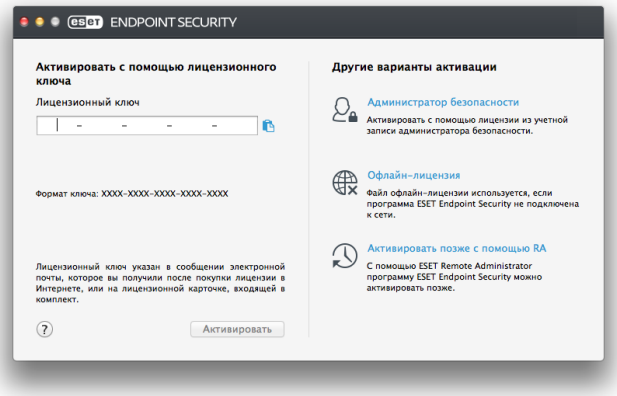
3.3.4 Удаленное обновление

Для установки новых версий ESET Endpoint Security используйте в Apple Remote Desktop команду **Установить пакеты**.

4. Активация программы

После завершения установки вам будет предложено активировать установленный продукт. Есть несколько способов активации. Доступность того или иного способа может зависеть от страны, а также от способа получения продукта (на компакт- или DVD-диске, с веб-страницы ESET и т. д.).

Чтобы активировать экземпляр ESET Endpoint Security непосредственно в приложении, щелкните значок ESET Endpoint Security, размещенный в строке меню macOS (в верхней части экрана), а затем щелкните элемент **Активация программы**. Активацию продукта можно выполнить также в главном меню. Для этого нужно последовательно выбрать элементы **Справка** > **Управление лицензией** или **Состояние защиты** > **Активировать продукт**.



Для активации ESET Endpoint Security можно воспользоваться любым из перечисленных ниже способов.

- **Активировать с помощью лицензионного ключа** - уникальная строка в формате XXXX-XXXX-XXXX-XXXX-XXXX, используемая для идентификации владельца и активации лицензии. Лицензионный ключ можно найти в сообщении электронной почты, полученном после приобретения программы, или на лицензионной карте в упаковке продукта.
- **Администратор безопасности**: учетная запись, созданная на портале ESET License Administrator с использованием учетных данных (адрес электронной почты и пароль). Этот способ позволяет централизовано управлять несколькими лицензиями.
- **Офлайн-лицензия** - автоматически созданный файл со сведениями о лицензии, который передается в продукт ESET. Файл офлайн-лицензии создается на портале ESET License Administrator и используется в средах, в которых приложение не может подключиться к центру лицензирования.

Кроме того, вы можете активировать клиент позже, если ваш компьютер находится в управляемой сети, а администратор планирует активировать программу с помощью ESET Remote Administrator.

ПРИМЕЧАНИЕ: Используя предоставленные администратором лицензии, приложение ESET Remote Administrator может активировать клиентские компьютеры в автоматическом режиме.

В ESET Endpoint Security версии 6.3.85.0 (и в более поздних версиях) можно активировать программу с помощью терминала. Для этого используйте следующую команду:

```
sudo ./esets_daemon --wait-respond --activate key=XXXX-XXXX-XXXX-XXXX-XXXX
```

Замените `XXXX-XXXX-XXXX-XXXX-XXXX` лицензионным ключом, который уже был использован для активации ESET Endpoint Security или зарегистрирован в ESET License Administrator. В результате выполнения команды отобразится состояние «OK» или сообщение об ошибке, если активация закончится неудачей.

5. Удаление

Запустить средство удаления ESET Endpoint Security можно двумя способами:

- Вставьте установочный CD/DVD-диск с программой ESET Endpoint Security в дисковод, откройте его на рабочем столе или в окне **Finder** и дважды щелкните элемент **Удалить**.
- Откройте установочный файл ESET Endpoint Security (*.dmg*) и дважды щелкните элемент **Удалить**.
- Запустите программу **Finder**, откройте папку **Приложения** на жестком диске, щелкните, удерживая клавишу CTRL, значок **ESET Endpoint Security**, а затем выберите команду **Показать содержимое пакета**. Откройте папку **Contents** > **Helpers** и дважды щелкните значок **Uninstaller**.

6. Краткий обзор интерфейса программы

Главное окно ESET Endpoint Security разделено на две основные части. Основное окно справа содержит информацию, относящуюся к параметру, выбранному в главном меню слева.

В главном меню доступны следующие разделы:

- **Состояние защиты**: отображается информация о состоянии файервола, защиты компьютера, контроля доступа в Интернет и защиты электронной почты.
- **Сканирование компьютера**: этот раздел позволяет настроить и запустить сканирование компьютера по требованию 14.
- **Обновление**: выводит информацию об обновлениях базы данных сигнатур вирусов.
- **Настройка**: этот раздел используется для настройки уровня безопасности компьютера.
- **Служебные программы**: этот раздел предоставляет доступ к файлам журналов 25, планировщику 27, карантину 29, запущенным процессам 31 и другим возможностям программы.
- **Справка**: обеспечивает доступ к файлам справки, базе знаний в Интернете, форме запроса на получение поддержки и дополнительной информации о программе.

6.1 Сочетания клавиш

Ниже перечислены сочетания клавиш, которые можно использовать при работе с программой ESET Endpoint Security.

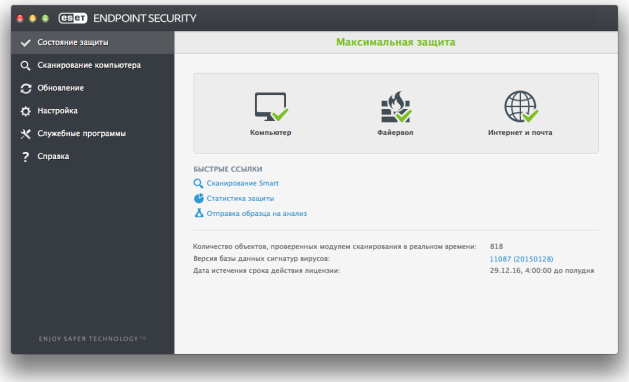
- *cmd+,* — отображение настроек ESET Endpoint Security.
- *cmd+O* — восстановление размера по умолчанию главного окна программы ESET Endpoint Security и его перемещение в центр экрана.
- *cmd+Q* — скрытие главного окна программы ESET Endpoint Security. Его можно открыть, щелкнув значок программы ESET Endpoint Security в строке меню macOS (вверху экрана).
- *cmd+W* — закрытие главного окна программы ESET Endpoint Security.

Перечисленные ниже сочетания клавиш работают, только если включен параметр **Использовать обычное меню** (**Настройка** > **Задать настройки приложения** > **Интерфейс**).

- *cmd+alt+L* — открытие раздела **Файлы журнала**.
- *cmd+alt+S* — открытие раздела **Планировщик**.
- *cmd+alt+Q* — открытие раздела **Карантин**.

6.2 Проверка работоспособности системы

Чтобы просмотреть состояние защиты, в главном меню щелкните элемент **Состояние защиты**. В основном окне появится сводная информация о работе модулей ESET Endpoint Security.



6.3 Устранение неполадок программы

Если модуль работает надлежащим образом, отображается зеленый флажок. В противном случае появляется красный восклицательный знак или оранжевый значок уведомления. Дополнительные сведения о модуле и рекомендуемое решение для устранения проблемы отображаются в главном окне программы. Чтобы изменить состояние отдельных модулей, щелкните синюю ссылку под каждым уведомлением.

Если предложенные решения не позволяют устранить проблему, можно попытаться найти решение в базе знаний ESET или обратиться в службу поддержки клиентов ESET. Служба поддержки быстро ответит на ваши вопросы и поможет решить любые проблемы с ESET Endpoint Security.

7. Защита компьютера

Конфигурацию компьютера можно найти в меню **Настройка** > **Компьютер**. Там отображается состояние параметра **Защита файловой системы в режиме реального времени**. Чтобы отключить отдельные модули, переключите их в состояние **ОТКЛЮЧЕНО**. Обратите внимание, что при этом защита компьютера может быть ослаблена. Чтобы открыть подробные параметры любого из модулей, нажмите кнопку **Настройка**.

7.1 Защита от вирусов и шпионских программ

Система защиты о вирусов обеспечивает защиту от вредоносных атак, изменяя файлы, которые потенциально представляют угрозу. При обнаружении вредоносного кода модуль защиты от вирусов и шпионских программ обезвреживает его,

блокируя его выполнение, а затем очищая, удаляя или помещая на карантин.

7.1.1 Общие параметры

В разделе **Общие** (**Настройка** > **Задать настройки приложения** > **Общие**) можно включить обнаружение приложений нескольких типов.

- **Потенциально нежелательные приложения**: не все потенциально нежелательные приложения являются вредоносными, однако они могут тем или иным образом снижать производительность системы. При установке такие приложения обычно запрашивают согласие пользователя. После их установки работа системы изменяется. Наиболее заметны такие изменения, как появление нежелательных всплывающих окон, запуск скрытых процессов, увеличение степени использования системных ресурсов, изменение результатов поисковых запросов и обмен данными с удаленными серверами.
- **Потенциально опасные приложения**: в эту категорию входит коммерческое законное программное обеспечение, которым могут воспользоваться злоумышленники, если такие приложения установлены без ведома пользователя. Это в том числе средства удаленного доступа, поэтому по умолчанию этот параметр отключен.
- **Подозрительные приложения**: к таким приложениям относятся программы, сжатые с помощью упаковщиков или средств защиты. Средства защиты такого типа часто используют злоумышленники, чтобы избежать обнаружения. Упаковщик — это самораспаковывающийся исполняемый файл, который может содержать несколько типов вредоносного ПО в одном пакете. Наиболее распространенными упаковщиками являются UPX, PE_Compact, PKLite и ASPack. При сжатии разными упаковщиками одно и то же вредоносное ПО может обнаруживаться по-разному. Также у упаковщиков есть способность с течением времени изменять свои сигнатуры, что усложняет обнаружение и удаление вредоносного ПО.

Чтобы настроить исключения для файловой системы или Интернета и почты 12, нажмите кнопку **Настройка**.

7.1.1.1 Исключения

В разделе Исключения можно исключить из сканирования определенные файлы, папки, приложения и адреса IP/IPv6.

Файлы и папки, указанные на вкладке **Файловая система**, будут исключены из сканирования для всех модулей: модуля сканирования при запуске, модуля сканирования в режиме реального времени и модуля сканирования по требованию (сканирование компьютера).

- **Путь**: путь к исключаемым файлам и папкам.
- **Угроза**: если рядом с исключаемым файлом указано имя угрозы, файл не проверяется только на предмет этой угрозы, а не всегда. Если файл окажется заражен другой вредоносной программой, модуль защиты от вирусов это обнаружит.
- [+]: создание нового исключения. Укажите путь к объекту (допускается использование подстановочных знаков *(звездочка) и ?(знак вопроса)) либо выберите папку или файл в структуре дерева.
- [−]: удаление выбранных записей.
- **По умолчанию**: отмена всех исключений.

На вкладке **Интернет и почта** из сканирования протоколов можно исключить определенные **приложения** и **адреса IP/IPv6**.

7.1.2 Защита при запуске

Функция проверки файлов при запуске предусматривает автоматическое сканирование файлов во время запуска системы. По умолчанию такое сканирование выполняется регулярно как запланированная задача после входа пользователя в систему и после успешного обновления базы данных вирусов. Чтобы изменить параметры модуля ThreatSense, которые влияют на сканирование при запуске системы, нажмите кнопку **Настройка**. Дополнительные сведения о настройке модуля ThreatSense приведены в этом разделе 16.

7.1.3 Защита файловой системы в режиме реального времени

Функция защиты файловой системы в режиме реального времени проверяет все типы носителей и запускает сканирование при наступлении различных событий. За счет использования технологии ThreatSense (описание приведено в разделе Настройка параметров модуля ThreatSense 16) защита файловой системы в режиме реального времени может быть разной для новых и уже существующих файлов. Для новых файлов защиту можно настроить более тонко.

По умолчанию все файлы сканируются при их **открытии**, **создании** и **исполнении**. Рекомендуется не изменять настройки по умолчанию, поскольку они обеспечивают максимальную защиту компьютера в режиме реального времени. Функция защиты в режиме реального времени запускается при загрузке системы и обеспечивает постоянное сканирование. В особых случаях (например, при возникновении конфликта с другим модулем сканирования в режиме реального времени) работу функции можно завершить, щелкнув значок ESET Endpoint Security, расположенный в строке меню (в верхней части экрана) и выбрав вариант **Отключить защиту файловой системы в реальном времени**. Кроме того, функцию защиты файловой системы можно отключить в главном окне программы: выберите **Настройка** > **Компьютер** и для параметра **Защита файловой системы в режиме реального времени** установите значение **ОТКЛЮЧЕНО**.

В модуле сканирования в режиме реального времени (Real-time) можно исключить следующие типы носителей.

- **Жесткие диски**: жесткие диски системы.
- **Съемные носители** — компакт-/DVD-диски, USB-устройства хранения, Bluetooth-устройства и т. п.
- **Сетевые носители**: все подключенные диски.

Рекомендуется оставить параметры по умолчанию, а изменять исключения из сканирования только в особых случаях (например, если сканирование определенных носителей приводит к значительному замедлению обмена данными).

Чтобы изменить дополнительные параметры защиты файловой системы, выберите меню **Настройка** > **Задать настройки приложения** (или нажмите *cmd+,*) > **Защита в режиме реального времени** и рядом с пунктом **Расширенные параметры** нажмите кнопку **Настройка** (описание приведено в разделе Расширенные параметры сканирования 13).

7.1.3.1 Расширенные параметры

В этом окне можно задать типы объектов, которые сканирует модуль ThreatSense. Дополнительную информацию о **самораспаковывающихся архивах**, **программах сжатия исполняемых файлов** и **расширенном эвристическом анализе** см. в разделе о настройках параметров модуля ThreatSense 16.

Изменять значения по умолчанию в разделе **Параметры архивов по умолчанию** не рекомендуется. Исключениями могут быть случаи, когда требуется устранить определенную проблему, поскольку увеличение уровня вложенности файлов в архиве может снизить производительность системы.

Параметры модуля ThreatSense для исполняемых файлов: по умолчанию **расширенный эвристический анализ** при исполнении файлов не применяется. Настоятельно рекомендуется включить ESET Live Grid и оптимизацию Smart, чтобы уменьшить воздействие на производительность системы.

Повысить совместимость сетевых томов: этот параметр повышает производительность при получении доступа к файлам в сети. Его следует включить, если при получении доступа к сетевым дискам понижается производительность. Эта функция использует координатор системных файлов в OS X 10.10 или более поздней версии. Помните, что не все приложения поддерживают координатор файлов, например Microsoft Word 2011 не поддерживает, а Word 2016 поддерживает.

7.1.3.2 Изменение параметров защиты в режиме реального времени

Защита в режиме реального времени является наиболее существенным элементом всей системы обеспечения безопасности. Изменять параметры модуля защиты в режиме реального времени следует с осторожностью. Это рекомендуется делать только в особых случаях, например при возникновении конфликтов с какими-либо приложениями или модулями сканирования в режиме реального времени, принадлежащими другим антивирусным программам.

После установки ESET Endpoint Security все параметры оптимизируются с целью обеспечения максимальной защиты системы. Чтобы восстановить параметры по умолчанию, нажмите кнопку **По умолчанию** в левом нижнем углу окна **Защита в режиме реального времени** (диалоговое окно **Настройка** > **Задать настройки приложения** > **Защита в режиме реального времени**).

7.1.3.3 Проверка защиты в режиме реального времени

Чтобы убедиться, что функция защиты в режиме реального времени работает и обнаруживает вирусы, воспользуйтесь тестовым файлом eicar.com. Это специальный безвредный файл, обнаруживаемый всеми программами защиты от вирусов. Он создан институтом EICAR (Европейский институт антивирусных компьютерных исследований) для тестирования функциональности антивирусных программ.

Чтобы проверить состояние защиты в режиме реального времени без использования программы ESET Remote Administrator, установите с помощью **терминала** удаленное подключение к клиентскому компьютеру, а затем выполните следующую команду:

```
/Applications/.esets/Contents/MacOS/esets_daemon --status
```

Отобразится состояние модуля сканирования в режиме реального времени: `RTPStatus=Enabled` или `RTPStatus=Disabled`.

При использовании терминала могут отображаться следующие сведения:

- установленная на клиентском компьютере версия программы ESET Endpoint Security;
- дата и версия базы данных сигнатур вирусов;
- путь к серверу обновлений.

ПРИМЕЧАНИЕ. Использование терминала рекомендуется только для опытных пользователей.

7.1.3.4 Устранение неполадок с неработающим модулем защиты в режиме реального времени

В этом разделе описаны проблемы, которые могут возникнуть с функцией защиты в режиме реального времени, а также способы их устранения.

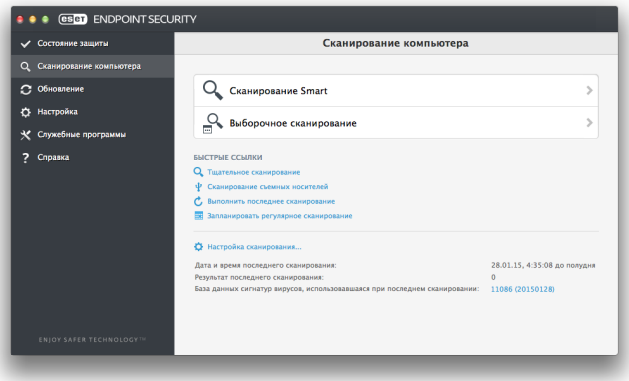
Защита в режиме реального времени отключена
Если защита в режиме реального времени была случайно отключена пользователем, ее нужно включить. Для этого щелкните в главном меню **Настройка** > **Компьютер** и установите для параметра **Защита файловой системы в режиме реального времени** значение **ВКЛЮЧЕНО**. Защиту файловой системы в режиме реального времени также можно включить в окне настроек приложения в разделе **Защита в режиме реального времени**, установив флажок **Включить защиту файловой системы в режиме реального времени**.

Функция защиты в режиме реального времени не обнаруживает и не обезвреживает вирусы
Убедитесь, что на компьютере не установлено другое антивирусное приложение. При одновременной работе двух систем защиты от вирусов в режиме реального времени могут возникать конфликты. Рекомендуется удалить все другие антивирусные приложения.

Защита в режиме реального времени не запускается
Если модуль защиты в режиме реального времени не инициализируется при запуске системы, это может быть вызвано конфликтом с другими программами. Если у вас возникла такая проблема, обратитесь за помощью в службу поддержки клиентов ESET.

7.1.4 Сканирование компьютера по требованию

При обнаружении симптомов возможного заражения компьютера (необычное поведение и т. п.) запустите **сканирование Smart**. Для обеспечения максимальной защиты сканирование компьютера следует выполнять регулярно, а не только при подозрении на заражение. Регулярное сканирование позволяет обнаружить вирусы, пропущенные модулем сканирования в режиме реального времени при их сохранении на диск. Это может произойти, если модуль сканирования в режиме реального времени был отключен или использовалась устаревшая база данных сигнатур вирусов.



Рекомендуется запускать сканирование компьютера по требованию хотя бы раз в месяц. Можно настроить сканирование так, чтобы оно запускалось по расписанию (**Служебные программы** > **Планировщик**).

Также можно перетаскивать выделенные файлы и папки с рабочего стола или из окна **Finder** на главный экран ESET Endpoint Security, значок Dock, значок в строке меню (в верхней части экрана) или значок приложения (в папке */Applications*).

7.1.4.1 Тип сканирования

Доступны два типа сканирования компьютера по требованию. **Сканирование Smart** позволяет быстро проверить систему без настройки каких-либо параметров. **Выборочное сканирование** позволяет выбрать профиль сканирования по умолчанию и указать объекты, которые нужно проверить.

7.1.4.1.1 Сканирование Smart

Режим сканирования Smart позволяет быстро запустить сканирование компьютера и очистить зараженные файлы без вмешательства пользователя. Главным преимуществом этого метода является простота использования и отсутствие необходимости детально настраивать параметры сканирования. Функция сканирования Smart проверяет все файлы во всех папках и автоматически очищает или удаляет обнаруженные заражения. При этом автоматически используется уровень очистки по умолчанию. Дополнительные сведения о типах очистки см. в разделе Очистка 17.

7.1.4.1.2 Выборочное сканирование

Выборочное сканирование позволяет указать параметры сканирования, такие как объекты и методы сканирования. Преимуществом этого типа сканирования является возможность детальной настройки параметров. Различные конфигурации можно сохранить в виде пользовательских профилей сканирования, которые полезны при регулярном сканировании с одинаковыми параметрами.

Чтобы указать объекты сканирования, последовательно выберите элементы **Сканирование компьютера** > **Выборочное сканирование** и отметьте в древовидной структуре нужные объекты. Объекты сканирования также можно определять более точно. Для этого укажите путь к подлежащей сканированию папке или файлу. Если нужно просканировать систему без применения очистки, выберите параметр **Сканировать без очистки**. Кроме того, в разделе **Настройка** > **Очистка** можно выбрать один из трех уровней очистки.

ПРИМЕЧАНИЕ. Пользователям, не имеющим достаточного опыта работы с антивирусными программами, не рекомендуется выполнять выборочное сканирование.

7.1.4.2 Объекты сканирования

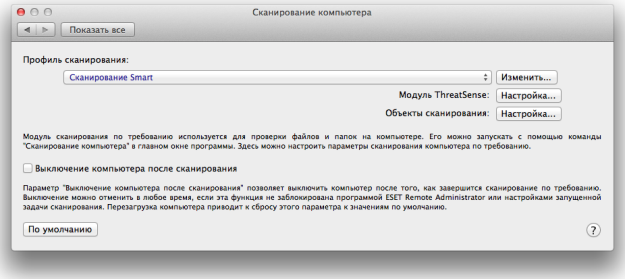
Дерево объектов сканирования позволяет выбирать файлы и папки, которые нужно проверить на наличие вирусов. Выбор папок может осуществляться также в соответствии с параметрами профиля.

Объекты сканирования можно определить более точно, введя путь к папкам или файлам, подлежащим сканированию. Выберите объекты сканирования в дереве, содержащем все доступные на компьютере папки. Для этого установите флажки возле нужных файлов и папок.

7.1.4.3 Профили сканирования

Предпочтительные настройки сканирования можно сохранить для использования в будущем. Для каждого регулярно используемого набора параметров рекомендуется создать отдельный профиль (с различными объектами, методами сканирования и т. д.).

Чтобы создать профиль, в главном меню выберите пункт **Настройка** > **Задать настройки приложения** (или нажмите сочетание клавиш *cmd+,*) > **Сканирование компьютера** и возле списка существующих профилей выберите команду **Изменить**.



Для создания профиля сканирования в соответствии с конкретными потребностями см. раздел Настройка параметров модуля ThreatSense 16, где описывается каждый параметр, используемый для настройки сканирования.

Пример: предположим, пользователю требуется создать собственный профиль сканирования, причем конфигурация сканирования Smart частично устраивает его, однако ему не нужно сканировать упаковщики или потенциально небезопасные программы и при этом необходимо применить тщательную очистку. В диалоговом окне **Список профилей модуля сканирования по требованию** введите имя профиля и нажмите кнопку **Добавить**, а затем — **ОК**. После этого задайте нужные параметры, настроив **модуль ThreatSense** и **объекты сканирования**.

Если после сканирования по требованию нужно отключить операционную систему и выключить компьютер, воспользуйтесь параметром **Выключение компьютера после сканирования**.

7.1.5 Настройка параметров модуля ThreatSense

ThreatSense — это собственная технология компании ESET, включающая в себя несколько сложных методов обнаружения угроз. Она является проактивной, т. е. защищает даже на ранних этапах распространения новых угроз. При этом используется сочетание нескольких методов (анализ кода, эмуляция кода, универсальные сигнатуры, сигнатуры вирусов), сочетание которых в значительной степени повышает уровень безопасности компьютера. Модуль сканирования способен контролировать несколько потоков данных одновременно, за счет чего увеличивается эффективность обнаружения угроз. Технология ThreatSense также эффективно предотвращает проникновение руткитов на компьютер.

Для модуля ThreatSense можно настроить несколько параметров сканирования:

- расширения и типы файлов, подлежащих сканированию;
- сочетание методов обнаружения угроз;
- уровни очистки и т. д.

Чтобы открыть окно настройки, выберите **Настройка > Задать настройки приложения...** (или нажмите *cmd+,*), а затем нажмите кнопку **Настройка...** модуля ThreatSense в модулях **Защита при запуске**, **Защита в режиме реального времени** и **Сканирование компьютера**, в которых используется технология ThreatSense (см. ниже). Разные сценарии обеспечения безопасности могут требовать различных настроек. Поэтому технологию ThreatSense можно настроить отдельно для каждого из перечисленных далее модулей защиты.

- **Защита при запуске**: автоматическая проверка файлов, выполняемая при запуске системы.
- **Защита в режиме реального времени**: защита файловой системы в режиме реального времени.
- **Сканирование компьютера**: сканирование компьютера по требованию.
- **Защита доступа в Интернет**
- **Защита электронной почты**

Параметры ThreatSense оптимизированы для каждого из модулей, и их изменение может существенно повлиять на работу системы. Например, если настроить параметры таким образом, чтобы упаковщики проверялись всегда или модуль защиты в режиме реального времени использовал расширенную эвристику, это может замедлить работу системы. В связи с этим рекомендуется не изменять используемые по умолчанию параметры ThreatSense для всех модулей, кроме модуля сканирования компьютера.

7.1.5.1 Объекты

В разделе **Объекты** можно указать файлы, которые необходимо проверять на предмет заражения.

- **Символические ссылки**: сканируются файлы, содержащие текстовую строку, которая интерпретируется и используется операционной системой как путь к другому файлу или каталогу (только для сканирования компьютера).
- **Почтовые файлы**: сканируются файлы электронной почты (недоступно для защиты в режиме реального времени).
- **Почтовые ящики**: сканируются почтовые ящики пользователя в системе (недоступно для защиты в режиме реального времени). Неправильное использование этого параметра может привести к конфликту с почтовым клиентом. Дополнительные сведения о преимуществах и недостатках применения этого параметра см. в статье базы знаний.
- **Архивы**: сканируются сжатые файлы в архивах с расширением RAR, ZIP, ARJ, TAR и т. д. (недоступно для защиты в режиме реального времени).
- **Самораспаковывающиеся архивы**: сканируются файлы, которые содержатся в самораспаковывающихся архивах (недоступно для защиты в режиме реального времени).
- **Упаковщики**: в отличие от стандартных архивов программы-упаковщики распаковывают файлы в системную память. При выборе этого параметра сканируются также стандартные статические упаковщики (например, UPX, yoda, ASPack, FGS).

7.1.5.2 Параметры

В разделе **Параметры** можно выбрать методы, которые будут использоваться при сканировании системы. Доступны следующие варианты:

- **Эвристический анализ**: эвристические алгоритмы анализируют активность программ на предмет вредоносных действий. Основным преимуществом эвристического анализа является возможность обнаруживать новое вредоносное программное обеспечение, сведения о котором еще не попали в базу данных сигнатур вирусов.
- **Расширенная эвристика**: метод основан на уникальном эвристическом алгоритме ESET, оптимизированном для обнаружения компьютерных червей и троянских программ, написанных на высокоуровневых языках программирования. Применение расширенной эвристики существенно улучшает возможности обнаружения вредоносных программ.

7.1.5.3 Очистка

Параметры очистки определяют способ очистки зараженных файлов модулем сканирования. В программе предусмотрено три уровня очистки.

- **Без очистки**: зараженные файлы не очищаются автоматически. Программа выводит предупреждение и предлагает пользователю выбрать нужное действие.
- **Стандартная очистка:** программа попытается автоматически очистить или удалить зараженный файл. Если автоматически выбрать правильное действие невозможно, программа предлагает сделать выбор пользователю. Выбор предоставляется и в том случае, если предварительно определенное действие не может быть выполнено.
- **Тщательная очистка**: программа очищает или удаляет все зараженные файлы, включая архивы. Единственное исключение — системные файлы. Если очистка файла невозможна, пользователь получает соответствующее уведомление и предложение выбрать требуемое действие.

Предупреждение. В стандартном режиме очистки, который используется по умолчанию, архив удаляется целиком только в том случае, если все файлы в нем заражены. Если архив содержит зараженные и незараженные файлы, он удален не будет. Если зараженный архив обнаружен в режиме тщательной очистки, он удаляется целиком, даже если в нем есть файлы без вредоносного кода.

7.1.5.4 Исключения

Расширением называется часть имени файла, отделенная от основной части точкой. Расширение указывает на тип и содержимое файла. Этот раздел параметров модуля ThreatSense позволяет определить типы файлов, которые не нужно сканировать.

По умолчанию сканируются все файлы независимо от их расширения. В список исключений можно добавить любое расширение. С помощью кнопок + и − можно разрешать и запрещать сканирование для тех или иных расширений.

Если сканирование определенных типов файлов препятствует нормальной работе программы, в некоторых случаях может потребоваться исключить такие файлы из сканирования. Например, рекомендуется исключить файлы *log*, *cfg* и *tmp*. Для ввода расширений используйте следующий формат:
log
cfg
tmp

7.1.5.5 Ограничения

В разделе **Ограничения** можно указать максимальный размер объектов и количество уровней вложенности для сканирования архивов.

- **Максимальный размер**: определяет максимальный размер сканируемых объектов. После установки ограничения модуль защиты от вирусов будет проверять только объекты, размер которых меньше указанного значения. Не рекомендуется изменять значение по умолчанию, если для этого нет особой причины. Он предназначен для опытных пользователей, которым необходимо исключить большие объекты из сканирования.
- **Максимальное время сканирования**: определяет максимальное время сканирования объекта. Если пользователь определил это значение, модуль защиты от вирусов прерывает сканирование текущего объекта по истечении указанного интервала времени независимо от того, завершено оно или нет.
- **Максимальный уровень вложенности**: определяет максимальную глубину сканирования архивов. Не рекомендуется изменять значение по умолчанию (10); в обычных условиях для этого нет особой причины. Если сканирование преждевременно прерывается из-за превышения уровня вложенности, архив остается непроверенным.
- **Максимальный размер файла**: определяет максимальный размер файлов в архиве (после извлечения), подлежащих сканированию. Если из-за этого ограничения сканирование прерывается до его завершения, архив остается непроверенным.

7.1.5.6 Другие настройки

Включить интеллектуальную оптимизацию
Когда включена оптимизация Smart, используются оптимальные настройки, обеспечивающие самый эффективный уровень сканирования без замедления его скорости. Разные модули защиты выполняют интеллектуальное сканирование с применением различных методов. Оптимизация Smart не определена в продукте жестким образом. Коллектив разработчиков компании ESET постоянно вносит в нее изменения, которые можно интегрировать в ESET Endpoint Security с помощью регулярных обновлений. Если оптимизация Smart отключена, при сканировании используются только пользовательские настройки ядра ThreatSense конкретного модуля.

Сканировать альтернативный поток данных
(применимо только к модулю сканирования по требованию)
Альтернативные потоки данных (ветвление ресурсов и данных), используемые файловой системой, представляют собой связи между файлами и папками, которые не видны для обычных методов сканирования. Многие вредоносные программы выдают себя за альтернативные потоки данных, чтобы избежать обнаружения.

7.1.6 Действия при обнаружении заражения

Вредоносный код может попасть в систему из разных источников: с веб-страниц, из общих папок, по электронной почте или со съемных носителей (USB-накопителей, внешних дисков, компакт- или DVD-дисков и т. п.).

Если наблюдаются признаки заражения компьютера (например, он стал медленнее работать, часто «зависает» и т. п.), рекомендуется выполнить действия, описанные ниже.

1. Щелкните элемент **Сканирование компьютера**.
2. Выберите параметр **Сканирование Smart** (дополнительную информацию см. в разделе Сканирование Smart 15).
3. По завершении сканирования просмотрите в журнале количество проверенных, зараженных и очищенных файлов.

Если нужно просканировать только определенную часть диска, выберите вариант **Выборочное сканирование** и укажите объекты, которые нужно просканировать на предмет наличия вирусов.

Чтобы понять в общих чертах, что происходит, когда программа ESET Endpoint Security выявляет заражение, представьте ситуацию, что модуль защиты файловой системы в режиме реального времени обнаружил заражение и в модуле настроен уровень очистки по умолчанию. Сначала модуль пытается очистить или удалить файл. Если действие по умолчанию для модуля защиты в режиме реального времени не определено, отобразится сообщение с предложением выбрать требуемое действие. Обычно на выбор предлагаются действия **Очистить**, **Удалить** и **Ничего не предпринимать**. Действие **Ничего не предпринимать** выбирать не рекомендуется, так как в этом случае зараженный файл останется в системе без изменений. Этот параметр предназначен для ситуаций, когда имеется полная уверенность, что файл безвреден и попал под подозрение по ошибке.

Очистка и удаление. Используйте очистку, если файл был атакован вирусом, добавившим в него вредоносный код. В этом случае в первую очередь файл следует попытаться очистить, чтобы восстановить его первоначальное состояние. Если файл содержит только вредоносный код, его следует удалить.

Удаление файлов из архивов. В режиме очистки по умолчанию архив удаляется целиком, только если он содержит исключительно зараженные файлы. Иначе говоря, архивы, в которых есть незараженные файлы, не удаляются. Сканирование в режиме **Тщательная очистка** следует применять с осторожностью, так как в этом режиме архив удаляется, если содержит хотя бы один зараженный файл независимо от состояния других файлов в архиве.

7.2 Защита доступа в Интернет и электронной почты

Чтобы открыть настройки защиты доступа в Интернет и электронной почты, в главном меню выберите пункт **Настройка** > **Интернет и почта**. Здесь можно также получить доступ к детальным настройкам каждого модуля, щелкнув параметр **Настройка**.

- **Защита доступа в Интернет**: отслеживает связь HTTP между веб-браузерами и удаленными серверами.
- **Защита почтового клиента**: позволяет контролировать обмен сообщениями по протоколам POP3 и IMAP.
- **Защита от фишинга**: блокирует потенциальные фишинговые атаки с веб-сайтов и доменов, которые компания ESET занесла в базу данных вредоносных программ.
- **Контроль доступа в Интернет**: блокирует веб-страницы, которые могут содержать неприемлемые или опасные материалы.

7.2.1 Защита доступа в Интернет

Функция защиты доступа в Интернет проверяет обмен данными между веб-браузерами и удаленными серверами на предмет соблюдения правил HTTP (протокола передачи гипертекста).

Чтобы настроить веб-фильтр, нужно указать номера портов для соединений HTTP 19 и/или URL-адреса 19.

7.2.1.1 Порты

На вкладке **Порты** можно указать номера портов, которые используются для обмена данными по протоколу HTTP. По умолчанию предварительно заданы номера портов 80, 8080 и 3128.

7.2.1.2 Списки URL-адресов

В разделе **Списки URL-адресов** можно указать HTTP-адреса, которые следует блокировать, разрешить или исключить из проверки. Веб-сайты из списка заблокированных адресов будут недоступны. К веб-сайтам из списка адресов, исключенных из проверки, доступ осуществляется без проверки на наличие вредоносного кода.

Чтобы разрешить доступ только к тем веб-сайтам, которые указаны в списке **Разрешенный URL-адрес**, установите флажок **Ограничить URL-адреса**.

Чтобы активировать список, установите рядом с его именем флажок **Включено**. Если вы хотите получать уведомление о том, что в адресную строку вводится адрес из текущего списка, установите флажок **С уведомлением**.

При создании списков URL-адресов можно использовать специальные символы *(звездочка) и ?(знак вопроса). Звездочка заменяет любую строку символов, а знак вопроса — любой символ. Особое внимание следует уделить при указании адресов, исключенных из проверки, поскольку этот список должен включать в себя только доверенные и надежные адреса. Аналогично, символы * и ? должны использоваться в этом списке надлежащим образом.

7.2.2 Защита электронной почты

Защита электронной почты позволяет контролировать обмен сообщениями через протоколы POP3 и IMAP. При проверке входящих сообщений программа использует все современные методы сканирования, которые обеспечивает модуль сканирования ThreatSense. Это означает, что обнаружение вредоносных программ происходит еще до сопоставления с базой данных сигнатур вирусов. Сканирование обмена сообщениями по протоколам POP3 и IMAP не зависит от используемого клиента электронной почты.

Модуль **ThreatSense: настройка**: расширенная настройка модуля антивирусного сканирования позволяет выбирать объекты сканирования, методы обнаружения и т. д. Нажмите кнопку **Настройка**, чтобы открыть окно расширенной настройки модуля сканирования.

Добавить уведомление к сообщениям электронной почты: после сканирования сообщения электронной почты можно добавить к нему уведомление, содержащее результаты сканирования. На эти уведомления нельзя полагаться полностью, поскольку они могут быть пропущены в проблематичных сообщениях в формате HTML или сфальсифицированы некоторыми вирусами. Доступны следующие варианты:

- **Никогда**: уведомления не добавляются.
- **Только к зараженным сообщениям**: помечаются как проверенные только сообщения, содержащие вредоносные программы.
- **Ко всем сканируемым сообщениям**: программа добавляет уведомления во все просканированные сообщения.

Добавлять примечание в поле темы полученных и прочитанных зараженных сообщений: установите этот флажок, если в тему зараженных сообщений необходимо добавлять предупреждения о вирусах, сгенерированные системой защиты электронной почты. Эта функция позволяет быстро фильтровать зараженные сообщения электронной почты. Она также повышает уровень доверия для получателя и, если обнаружено заражение, предоставляет ценную информацию об уровне угрозы данного письма или отправителя.

Шаблон, добавляемый в поле темы зараженных сообщений: отредактируйте этот шаблон, если требуется изменить формат префикса темы для зараженных писем.

В нижней части этого окна можно также включить или отключить проверку обмена данными по электронной почте по протоколу POP3 или IMAP. Дополнительные сведения см. в следующих темах:

- Проверка протокола POP3 20
- Проверка протокола IMAP 20

7.2.2.1 Проверка протокола POP3

Протокол POP3 является самым распространенным протоколом, используемым для получения сообщений в клиентских приложениях для работы с электронной почтой. Программа ESET Endpoint Security обеспечивает защиту для этого протокола независимо от того, какой клиент электронной почты используется.

Модуль защиты, обеспечивающий такой контроль, автоматически запускается при запуске системы и остается активным в памяти. Чтобы модуль работал правильно, убедитесь, что проверка протокола POP3 включена. Контроль протокола POP3 осуществляется автоматически без необходимости перенастройки почтового клиента. По умолчанию сканируются все данные, проходящие через порт 110, но при необходимости можно добавить и другие порты. Номера портов следует разделять запятой.

Если параметр **Включить проверку протокола POP3** включен, весь трафик по протоколу POP3 отслеживается с целью обнаружения вредоносных программ.

7.2.2.2 Проверка протокола IMAP

Протокол IMAP (IMAP) — это еще один интернет-протокол для получения электронной почты, который имеет определенные преимущества перед POP3. Например, сразу несколько клиентов могут одновременно подключаться к одному и тому же почтовому ящику и передавать сведения о состоянии сообщения, в частности сведения о том, что сообщение было прочитано, удалено или на него был дан ответ. Программа ESET Endpoint Security обеспечивает защиту этого протокола вне зависимости от используемого почтового клиента.

Модуль защиты, обеспечивающий такой контроль, автоматически запускается при запуске системы и остается активным в памяти. Чтобы модуль работал правильно, убедитесь, что проверка протокола IMAP включена. Контроль протокола IMAP осуществляется автоматически без необходимости перенастройки почтового клиента. По умолчанию сканируются все данные, проходящие через порт 143, но при необходимости можно добавить и другие порты. Номера портов следует разделять запятой.

Если параметр **Включить проверку протокола IMAP** включен, весь трафик по протоколу IMAP отслеживается с целью обнаружения вредоносных программ.

7.3 Защита от фишинга

Термином *фишинг* обозначается преступная деятельность с использованием приемов социотехники (манипулирование пользователями для получения конфиденциальной информации). Фишинг часто используется для получения доступа к такой конфиденциальной информации, как номера банковских счетов, номера кредитных карт, PIN-коды или имена пользователей и пароли.

Функцию защиты от фишинга не рекомендуется выключать (**Настройка** > **Задать настройки приложения** > **Защита от фишинга**). Все потенциальные фишинговые атаки с веб-сайтов или доменов, занесенных компанией ESET в базу данных вредоносного ПО, блокируются, после чего отображается уведомление об атаке.

8. Файервол

Персональный файервол контролирует весь входящий и исходящий сетевой трафик, разрешая или запрещая (на основе заданных правил фильтрации) те или иные сетевые подключения. Он обеспечивает защиту от атак с удаленных компьютеров и позволяет блокировать некоторые службы. Он также предоставляет защиту от вирусов для протоколов HTTP, POP3 и IMAP.

Конфигурацию персонального файервола можно найти в меню **Настройка** > **Файервол**. Здесь можно настроить режим, правила и параметры фильтрации. Здесь также доступны более детальные настройки программы.

Если включить параметр **Блокировать весь сетевой трафик: отключить сеть**, персональный файервол будет блокировать все входящие и исходящие подключения. Используйте этот параметр только в особых случаях, когда возникает опасная критическая ситуация, требующая немедленного отключения системы от сети.

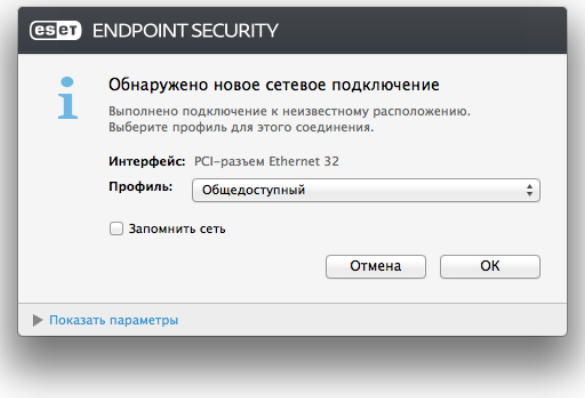
8.1 Режимы фильтрации

В персональном файерволе ESET Endpoint Security есть три режима фильтрации. Параметры режимов фильтрации можно настроить, последовательно выбрав элементы «Настройка» > «**Дополнительные настройки...**». > **Файервол**. Работа файервола меняется в зависимости от выбранного режима. Режимы фильтрации влияют также на уровень взаимодействия с пользователем.

Весь трафик блокируется: блокируется весь входящий и исходящий трафик.

Автоматически с исключениями: режим по умолчанию. Этот режим подходит пользователям, которые предпочитают простую и удобную работу с файерволом без необходимости определять правила. В автоматическом режиме разрешен стандартный исходящий трафик для данной системы и блокируются соединения, не инициированные со стороны сети. Также можно добавить настраиваемые, пользовательские, правила.

Интерактивный режим: в этом режиме можно создать пользовательскую конфигурацию персонального файервола. При обнаружении подключения, которое не подпадает ни под одно из существующих правил, отображается сообщение о неизвестном подключении. В окне этого сообщения подключение можно запретить или разрешить и на основе принятого решения создать на будущее правило. После создания нового правила все будущие подключения этого типа будут разрешены или запрещены в зависимости от параметров правила.



Если необходимо записывать подробную информацию обо всех заблокированных подключениях в файл журнала, выберите параметр **Регистрировать все заблокированные соединения**. Чтобы просмотреть файлы журналов файервола, в главном меню последовательно щелкните элементы **Служебные программы** > **Журналы** и в раскрывающемся меню **Журнал** выберите пункт **Файервол**.

8.2 Правила файервола

Правило содержит набор условий, которые позволяют проверять все сетевые подключения и выполнять необходимые действия в соответствии с этими условиями. В правиле персонального файервола можно определить действие, которое должно выполняться при установке обозначенного в правиле подключения.

Входящее подключение инициируется удаленным компьютером, который пытается установить соединение с локальной системой. Исходящее подключение работает по обратному принципу — локальная система обращается к удаленному компьютеру.

Обнаружив новое неизвестное подключение, хорошо подумайте, прежде чем разрешать или запрещать его. Незапрошенное, незащищенное или неизвестное подключение может подвергнуть систему опасности. Если такое подключение установлено, рекомендуем обратить особое внимание на удаленный компьютер и приложение, которое пытается подключиться к вашему компьютеру. При многих видах заражений осуществляются попытки получения и отправки конфиденциальных данных и загрузки других вредоносных приложений на рабочие станции. Персональный файервол позволяет обнаружить и разорвать такие подключения.

По умолчанию программы, подписанные компанией Apple, получают автоматический доступ к сети. Если необходимо отключить эту функцию, снимите флажок **Разрешить программам, подписанным Apple, автоматический доступ к сети**.

8.2.1 Создание правил

На вкладке **Правила** содержится список всех правил, которые применяются в отношении трафика отдельных приложений. Правила добавляются автоматически в соответствии с реакциями пользователя на новое соединение.

1. Чтобы создать правило, нажмите кнопку **Добавить** , введите имя правила и перетащите значок приложения в пустое поле (или нажмите кнопку **Обзор**, чтобы найти приложение в папке */ Applications*). Чтобы применить правило ко всем приложениям, установленным на компьютере, выберите элемент **Все приложения**.
2. В следующем окне необходимо указать **действие** (разрешить или запретить обмен данными между выбранным приложением и сетью) и **направление** подключения (входящее, исходящее или оба направления). Установите флажок **Правило журнала**, чтобы записывать в журнал сведения о всех подключениях, к которым относится это правило. Чтобы просмотреть журналы файервола, в главном меню ESET Endpoint Security щелкните **Служебные программы** > **Журналы** и в раскрывающемся списке **Журнал** выберите пункт **Файервол**.
3. В разделе **Протоколы и порты** настройте протокол и порт, которые приложение использует для обмена данными (если выбран протокол TCP или UDP). На уровне транспортного протокола обеспечивается безопасная и эффективная передача данных.
4. Наконец, укажите критерии **назначения** (IP-адрес, диапазон, подсеть, сеть Ethernet или Интернет) для правила.

8.3 Зоны файервола

Зона представляет собой набор сетевых адресов, которые составляют одну логическую группу. Каждому адресу в группе назначаются похожие правила, определенные централизовано для всей группы.

Чтобы создать зону, нажмите кнопку **Добавить**. Введите **имя** и **описание** (необязательно) зоны, выберите профиль, к которому будет принадлежать данная зона, и укажите адрес IPv4/IPv6, диапазон адресов, подсеть, сеть Wi-Fi или интерфейс.

8.4 Профили файервола

С помощью **профилей** можно контролировать работу персонального файервола ESET Endpoint Security. Создавая или изменяя правило для персонального файервола, можно назначить его для какого-либо конкретного профиля. При выборе профиля применяются только общие правила (без указания профиля) и правила, назначенные непосредственно для этого профиля. Можно создать несколько профилей с различными правилами, чтобы можно было легко изменять работу персонального файервола.

8.5 Журналы файервола

Персональный файервол ESET Endpoint Security сохраняет сведения обо всех важных событиях в файл журнала. Чтобы получить доступ к журналам файервола, в главном меню последовательно щелкните элементы **Служебные программы** > **Журналы** и в раскрывающемся меню **Журнал** выберите пункт **Файервол**.

Файлы журналов помогают обнаруживать ошибки и вторжения в систему. Журналы персонального файервола ESET содержат следующие сведения:

- дата и время события;
- имя события;
- источник;
- сетевой адрес целевого объекта;
- сетевой протокол связи;
- примененное правило;
- используемое приложение;
- пользователь.

Тщательный анализ этих данных может помочь обнаружить попытки нарушения безопасности системы. На потенциальную угрозу указывают многие другие факторы, защиту от которых можно обеспечить с помощью персонального файервола. Среди этих факторов можно назвать частые подключение с неизвестных компьютеров, множественные попытки установить соединение, сетевая активность неизвестных приложений или использование неизвестных номеров портов.

9. Контроль устройств

С помощью ESET Endpoint Security можно сканировать, блокировать и изменять расширенные фильтры и/или разрешения, а также указывать, может ли пользователь получать доступ к конкретному устройству и работать с ним. Это удобно, если администратор компьютера хочет предотвратить использование устройств, на которых присутствует нежелательное содержимое.

Поддерживаемые внешние устройства:
- Дисковый накопитель (жесткий диск, USB-устройство флэш-памяти)
- Компакт-/DVD-диск
- USB-принтер
- Устройство обработки изображений
- Последовательный порт
- Сеть
- Портативное устройство

При подключении устройства, заблокированного существующим правилом, отобразится окно оповещения, и доступ к устройству будет заблокирован.

В журнале контроля устройств записываются все происшествия, запускающие функцию контроля устройств. Записи журнала можно просмотреть в главном окне программы ESET Endpoint Security в разделе **Служебные программы** > **Файлы журнала** 25.

9.1 Редактор правил

Параметры функции контроля устройств можно изменить в меню **Настройка** > **Задать настройки приложения...** > **Контроль устройств**.

Если щелкнуть параметр **Включить контроль устройств**, в ESET Endpoint Security будет активирована функция контроля устройств. Как только контроль устройств будет включен, вы сможете управлять ролями контроля устройств и изменять их. Чтобы включить и выключить правило, используйте флажок рядом с его именем.

Для добавления или удаления правил используйте кнопки  и  . Правила приведены в порядке их приоритета: имеющие более высокий приоритет правила располагаются выше. Чтобы изменить порядок, достаточно перетащить правило на новое место или щелкнуть  и выбрать нужный параметр.

ESET Endpoint Security автоматически обнаруживает все подключенные устройства и их параметры (тип устройства, производитель, модель, серийный номер). Вместо того чтобы создавать правила вручную, щелкните параметр **Заполнить**, выберите устройство и нажмите кнопку **Продолжить**, чтобы создать правило.

Некоторые устройства можно разрешить или заблокировать на основании сведений об их пользователе, группе пользователей или в соответствии с несколькими дополнительными параметрами, которые задаются в конфигурации правил. В списке правил содержится несколько описаний для каждого правила. в том числе имя, тип устройства, серьезность регистрируемых событий и действие, подлежащее выполнению после подключения устройства к компьютеру.

Имя

Чтобы упростить идентификацию правила, введите его описание в поле **Имя**. Чтобы включить или отключить это правило, установите или снимите флажок **Правило включено**. Это может быть полезно в том случае, если вы не хотите полностью удалять правило.

Тип устройства

Выберите нужный тип внешнего устройства в раскрывающемся меню. Сведения о типе устройства поступают из операционной системы. К запоминающим устройствам относятся внешние диски и традиционные устройства чтения карт памяти, подключенные с помощью интерфейса USB или FireWire. Примерами устройств обработки изображений служат сканеры и камеры. Поскольку эти устройства предоставляют сведения только о своих действиях, а не о пользователях, заблокировать их можно только глобально.

Действие

Доступ к устройствам, не предназначенным для хранения данных, можно только разрешить или заблокировать. А вот правила для запоминающих устройств позволяют выбрать одно из указанных ниже прав.

Чтение и запись: будет разрешен полный доступ к устройству.

Только чтение: будет разрешено только чтение данных с устройства.

Блокировать: доступ к устройству будет заблокирован.

Тип критериев

Выберите элемент **Группа устройств** или **Устройство**. С помощью указанных ниже дополнительных параметров можно точно настраивать и изменять правила для конкретных устройств.

Производитель: фильтрация производителей по имени или идентификатору.

Модель: наименование устройства.

Серийный номер: у внешних устройств обычно есть серийные номера. Если речь идет о компакт- или DVD-диске, то это серийный номер конкретного носителя, а не дисковода компакт- или DVD-дисков.

ПРИМЕЧАНИЕ. Если для этих параметров не заданы значения, во время сопоставления правило игнорирует эти поля. Для параметров фильтрации во всех текстовых полях не учитывается регистр и не поддерживаются подстановочные знаки (*, ?).

ПОДСКАЗКА. Для просмотра сведений об устройстве создайте правило для соответствующего типа устройства и подключите устройство к компьютеру. После подключения устройства сведения о нем отобразятся в журнале контроля устройств 25.

Серьезность регистрируемых событий

Всегда: записываются все события.

Диагностика: записывается информация, необходимая для тщательной настройки программы.

Информация: записываются информативные сообщения, а также все перечисленные выше сведения.

Предупреждение: записывается информация обо всех критических ошибках и предупреждениях.

Ничего: журналы не создаются.

Список пользователей

Правила можно назначать только для некоторых пользователей или их групп, добавленных в список пользователей.

Изменить...: открывается компонент **Редактор удостоверений**, в котором можно выбирать пользователей или группы. Чтобы создать список пользователей, в левой части окна в списке **Пользователи** выберите пользователей и нажмите кнопку **Добавить**. Чтобы удалить пользователя, в списке **Выбранные пользователи** выберите имя пользователя и нажмите кнопку **Удалить**. Чтобы отобразить всех пользователей системы, установите флажок **Показывать всех пользователей**. Если этот список пуст, все пользователи получат разрешения.

ПРИМЕЧАНИЕ. Не все устройства можно фильтровать по пользовательским правилам (например, устройства обработки изображений предоставляют информацию только о действиях, но не о пользователях).

10. Контроль доступа в Интернет

Функция **Контроль доступа в Интернет** используется для настройки параметров, которые защитят вашу компанию от опасности юридических исков. Данная функция может управлять доступом к веб-сайтам, которые нарушают права на интеллектуальную собственность. Цель заключается в предотвращении доступа сотрудников к страницам с неприемлемым или опасным содержимым, а также к ресурсам, посещение которых может отрицательно сказаться на эффективности работы. Работодатели или системные администраторы могут запретить доступ к более чем 27 предварительно заданным категориям веб-сайтов, включающим свыше 140 подкатегорий.

Контроль доступа в Интернет по умолчанию отключен. Чтобы включить его, выберите **Настройка** > **Задать настройки приложения** > **Контроль доступа в Интернет** и установите флажок **Включить контроль доступа в Интернет**.

В редакторе правил отображаются существующие правила, созданные на основе URL-адресов или категорий. В списке правил представлен ряд описаний правил, например имя, тип блокирования, действие, подлежащее выполнению при срабатывании правила контроля доступа в Интернет, а также серьезность для журнала 25.

Чтобы создать правило, нажмите кнопку  . Дважды щелкните поле **Имя** и введите описание правила, чтобы упростить его идентификацию.

Флажок **Включено** позволяет включить или отключить правило. Это может пригодится в тех случаях, когда правило нужно отключить на время, а не удалять безвозвратно.

Тип

Действие на основе URL-адреса: доступ к определенному веб-сайту. Дважды щелкните поле **URL-адрес или категория** и укажите требуемый URL-адрес.
В списке URL-адресов нельзя использовать специальные символы * (звездочка) и ? (вопросительный знак). Адреса веб-страниц с несколькими доменами верхнего уровня необходимо вводить вручную (*examplepage.com* , *examplepage.sk* и т. д.). При внесении домена в список все содержимое, расположенное в нем и во всех поддоменах (например, *sub. examplepage.com*), будет разрешено или заблокировано в зависимости от действия на основе URL-адреса.
Действие на основе категории: дважды щелкните поле **URL-адрес или категория** и выберите соответствующие категории.

Удостоверение

Позволяет выбрать пользователей, к которым будет применяться правило.

Права доступа

Разрешить: к URL-адресу или категории будет предоставлен доступ.
Блокировать: URL-адрес или категория будет блокироваться.

Серьезность (для фильтрации 26 файлов журнала).

Всегда: записываются все события.
Диагностика: записывается информация, необходимая для тщательной настройки программы.
Информация: записываются информативные сообщения, а также все перечисленные выше сведения.
Предупреждение: записывается информация обо всех критических ошибках и предупреждениях.
Нет: журналы не будут создаваться.

11. Служебные программы

В меню **Сервис** находятся модули, которые облегчают администрирование программы и предлагают дополнительные параметры для опытных пользователей.

11.1 Файлы журналов

Файлы журнала содержат информацию о всех важных программных событиях, которые произошли, и предоставляют общие сведения об обнаруженных угрозах. Ведение журналов является важнейшим средством анализа системы, обнаружения угроз и устранения неполадок. Оно выполняется в фоновом режиме без вмешательства пользователя. Данные сохраняются в соответствии с текущими параметрами степени детализации журналов. Просматривать текстовые сообщения и файлы журналов, а также архивировать их можно непосредственно в среде ESET Endpoint Security.

Получить доступ к файлам журналов можно из главного окна ESET Endpoint Security (**Служебные программы** > **Файлы журналов**). В раскрывающемся меню **Журнал** в верхней части окна выберите нужный тип журнала. Доступны такие журналы:

1. **Обнаруженные угрозы**: сведения о событиях, связанных с обнаруженными заражениями.
2. **События**: в журнале событий регистрируются все важные действия, выполняемые программой ESET Endpoint Security.
3. **Сканирование компьютера**. В этом окне отображаются результаты всех выполненных операций сканирования. Чтобы получить подробную информацию о той или иной операции сканирования компьютера, дважды щелкните соответствующую запись.

4. **Контроль устройств**: содержит список подключенных к компьютеру съемных носителей и устройств. В файл журнала записываются только устройства с правилом контроля устройств. Если правило не совпадает с подключенным устройством, запись о нем в журнале не создается. Также здесь отображаются такие сведения, как тип устройства, серийный номер, имя производителя и размер носителя (при его наличии).
5. **Файервол**. В журнале событий файервола отображаются все попытки удаленных атак, которые обнаружил персональный файервол. В журналах файервола содержатся сведения об обнаруженных атаках на ваш компьютер. В столбце **Событие** представлены сведения об обнаруженных атаках, в столбце **Источник** содержится информация о злоумышленнике, а в столбце **Протокол** перечисляются протоколы обмена данными, которые использовались для атаки.
6. **Контроль доступа в Интернет**. Содержит список заблокированных или разрешенных URL-адресов и сведения об их группировке по категориям.
7. **Отфильтрованные веб-сайты**: этот список используется для просмотра списка веб-сайтов, заблокированных функцией защиты доступа в Интернет 19. иликонтроля доступа в Интернет 24. В этих журналах отображается время, URL-адрес, состояние, IP-адрес, пользователь и приложение, с помощью которого установлено соединение с тем или иным веб-сайтом.

Чтобы скопировать содержимое файла журнала в буфер обмена, щелкните файл правой кнопкой мыши и выберите пункт **Копировать**.

11.1.1 Обслуживание журналов

Попасть в раздел настроек ведения журналов ESET Endpoint Security можно из главного окна приложения. Для этого последовательно щелкните **Настройка** > **Задать настройки приложения** > **Служебные программы** > **Файлы журналов**. Для файлов журналов можно настроить несколько параметров.

- **Автоматически удалять устаревшие записи журнала**: записи в журнале старше указанного времени (в днях) будут автоматически удаляться.
- **Оптимизировать файлы журналов автоматически**: включает автоматическую дефрагментацию файлов журналов при превышении указанной процентной доли неиспользуемых записей.

Всю важную информацию, отображаемую в окнах программы, а также сообщения об угрозах и событиях можно сохранять в удобочитаемых текстовых форматах, например в формате обычного текста или CSV (данные с разделителями-запятыми). Если необходимо сделать эти файлы доступными для обработки в сторонних приложениях, установите флажок **Включить запись журналов в текстовые файлы**.

Чтобы указать целевую папку для сохранения файлов журналов, рядом с элементом **Дополнительные настройки** нажмите кнопку **Настройка**.

В зависимости от настроек в разделе **Текстовые файлы журнала: изменить** можно сохранять журналы с записью следующих данных.

- Такие события, как *Неверное имя пользоват еля и пароль*, *Не удает ся обновит ь базу данных сигнат ур вирусов* и т. д., записываются в файл *eventslog.txt*.
- Угрозы, обнаруженные модулями сканирования при запуске системы, защиты в режиме реального времени и сканирования компьютера, сохраняются в файле с именем *threatslog.txt*.
- Результаты всех выполненных сканирований сохраняются в формате *scanlog.НОМЕР.txt*.
- Устройства, которые блокирует функция контроля доступа в Интернет, заносятся в файл devctllog.txt
- Все события, имеющие отношение к обмену данными через файервол, записываются в файл firewalllog.txt
- Веб-страницы, которые блокирует функция контроля доступа в Интернет, заносятся в файл webctllog.txt

Чтобы настроить фильтр **записей журнала сканирования компьютера по умолчанию**, нажмите кнопку **Изменить** и выберите нужные типы журналов. Дополнительные сведения об этих типах журналов см. в разделе Фильтрация журнала 26.

11.1.2 Фильтрация журнала

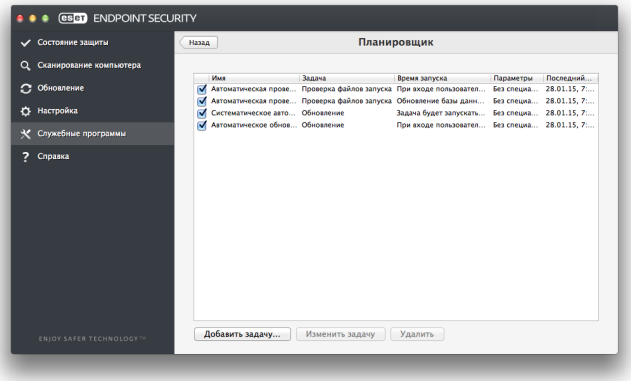
В журналах хранится информация о важных системных событиях. Функция фильтрации журнала позволяет отобразить записи только об определенных событиях.

Ниже указаны типы журналов, используемые чаще всего.

- **Критические предупреждения**: в эти журналы записываются критические системные ошибки (например, сбой запуска модуля защиты от вирусов).
- **Ошибки**: в эти журналы записываются сообщения об ошибках, такие как *Не удалось загрузит ь ф айл* , и критические ошибки.
- **Предупреждения**: в эти журналы записываются сообщения с предупреждениями.
- **Информационные записи**: в эти журналы записываются информационные сообщения, в том числе сообщения о выполненных обновлениях, предупреждения и т. д.
- **Диагностические записи**: в эти журналы записываются данные, необходимые для точной настройки программы, а также все описанные выше записи.

11.2 Планировщик

Планировщик можно найти в главном меню ESET Endpoint Security в разделе **Служебные программы**. Здесь приведен полный список запланированных задач и параметры их запуска (дата, время и используемый профиль сканирования).



Планировщик управляет запланированными задачами и запускает их по расписанию с предварительно заданными параметрами и свойствами. Параметры и свойства задач содержат такую информацию, как дата и время выполнения задачи, а также используемые при этом профили.

В планировщике по умолчанию отображаются следующие запланированные задачи.

- Обслуживание журналов (после установки флажка **Показывать системные задачи** в настройках планировщика).
- Проверка файлов при входе пользователя.
- Проверка файлов после обновления базы данных сигнатур вирусов.
- Регулярное автоматическое обновление.
- Автоматическое обновление после входа пользователя в систему.

Чтобы изменить конфигурацию имеющейся запланированной задачи (как заданной по умолчанию, так и созданной пользователем), щелкните ее, удерживая нажатой клавишу CTRL, и выберите в контекстном меню команду **Изменить** (или выделите задачу и нажмите кнопку **Изменить задачу**).

11.2.1 Создание задач

Чтобы создать задачу в планировщике, нажмите кнопку **Добавить задачу** или щелкните в пустом поле, удерживая клавишу CTRL, и выберите в контекстном меню команду **Добавить**. Доступны пять типов запланированных задач.

- **Запуск приложения.**
- **Обновление.**
- **Обслуживание журналов.**
- **Сканирование компьютера по требованию.**
- **Проверка файлов, исполняемых при запуске системы.**

ПРИМЕЧАНИЕ. Выбрав задачу **Запуск приложения**, вы сможете запускать программы в качестве системного пользователя с именем nobody. Разрешения на запуск приложений с помощью планировщика определяются операционной системой macOS.

В приведенном ниже примере планировщик используется для добавления новой задачи обновления, поскольку обновление — это одна из наиболее часто используемых запланированных задач.

1. В раскрывающемся меню **Запланированная задача** выберите пункт **Обновление**.
2. В поле **Имя задачи** введите имя задачи.

3. В раскрывающемся меню **Запуск задачи** укажите частоту выполнения задачи. В зависимости от указанной частоты запуска будет предложено указать различные параметры обновления. Если выбран вариант **Определяется пользователем**, вам будет предложено указать дату и время в формате *cron* (дополнительные сведения см. в разделе Создание пользовательской задачи 28).
4. Затем укажите, какое действие следует предпринимать, если задача не может быть выполнена в установленное время.
5. Нажмите кнопку **Готово**. Новая задача появится в списке запланированных.

В программе ESET Endpoint Security предусмотрены уже готовые запланированные задачи, которые обеспечивают правильную работу приложения. Изменить эти задачи нельзя, и по умолчанию они скрыты. Чтобы эти задачи отображались, в главном меню последовательно щелкните элементы **Настройка** > **Задать настройки приложения** > **Планировщик** и установите флажок **Показывать системные задачи**.

11.2.2 Создание пользовательской задачи

Выбрав в раскрывающемся списке «Запустить задачу» тип «Определяется пользователем», нужно дополнительно указать несколько специальных параметров.

Дату и время **пользовательской** задачи необходимо указывать в формате CRON с расширенным значением года (строка из шести полей, разделенных пробелами):

```
минута (0-59) час (0-23) число месяца (1-31)
месяц (1-12) год (1970-2099) день недели (0-7,
воскресенье — 0 или 7)
```

Например:

```
30 6 22 3 2012 4
```

В CRON-выражениях допускается использование следующих специальных символов:

- звездочка (`*`): выражение соответствует всем значениям поля (например, звездочка в третьем поле — число месяца — означает любое число);
- дефис (`-`): задает диапазон, например `3-9`
- запятая (`,`): разделяет элементы списка, например `1,3,7,8`
- косая черта (`/`): задает шаг диапазона, например `3-28/5` в третьем поле (число месяца) означает третье число месяца, а также другие числа с шагом пять дней.

Использовать названия дней (Monday-Sunday) и месяцев (January-December) нельзя.

ПРИМЕЧАНИЕ. Если заданы число месяца и день недели, команда выполняется только в случае совпадения значений по обоим полям.

11.3 Live Grid

Система своевременного обнаружения Live Grid позволяет компании ESET постоянно и без промедления получать информацию о новых заражениях. Двунаправленная система своевременного обнаружения Live Grid создана с единственной целью — улучшить предлагаемую пользователям защиту. Лучший способ получать информацию о новых угрозах сразу же после их появления — это поддержание связи с максимально возможным количеством пользователей и использование полученных от них данных для постоянного обновления баз данных сигнатур вирусов. В настройках Live Grid пользователи могут выбрать один их двух вариантов действий.

1. Систему своевременного обнаружения Live Grid можно не включать. Функциональность программного обеспечения при этом не ограничивается, но в некоторых случаях ESET Endpoint Security может быстрее обрабатывать новые угрозы, чем обновление базы данных сигнатур вирусов.
2. Систему своевременного обнаружения Live Grid можно настроить для отправки анонимной информации о новых угрозах и объектах, содержащих вредоносный код. Эта информация отправляется в компанию ESET для подробного анализа. Исследование этих угроз помогает компании ESET обновлять базу данных угроз и улучшать средства их обнаружения.

Система своевременного обнаружения Live Grid будет собирать информацию о компьютере, которая имеет отношение к новым обнаруженным угрозам. Она может включать образец кода или копию файла, в котором была обнаружена угроза, путь к файлу, его имя, дату и время обнаружения угрозы, имя процесса, в котором она обнаружена, и версию операционной системы пользователя.

Существует риск, что некоторая информация о вас или вашем компьютере (имя пользователя в пути к каталогу и т. п.) может случайно стать доступной для сотрудников лаборатории ESET. Тем не менее эта информация будет использоваться ИСКЛЮЧИТЕЛЬНО для того, чтобы помочь нам незамедлительно реагировать на появление новых угроз.

Чтобы открыть настройки Live Grid, в главном меню выберите пункт **Настройка** > **Задать настройки приложения** > **Live Grid**. Установите флажок **Включить систему репутации ESET Live Grid (рекомендуется)**, чтобы активировать Live Grid, а затем рядом с пунктом **Расширенные параметры** нажмите кнопку **Настройка**.

11.3.1 Подозрительные файлы

По умолчанию программа ESET Endpoint Security отправляет подозрительные файлы в лабораторию ESET по изучению угроз для тщательного анализа. Если вы не хотите, чтобы такие файлы отправлялись автоматически, снимите флажок **Отправка подозрительных файлов** (**Настройка** > **Задать настройки приложения** > **Live Grid** > **Настройка**).

При обнаружении подозрительного файла его можно отправить в нашу лабораторию для анализа. Для этого в главном окне программы выберите **Служебные программы** > **Отправить файл на анализ** . Если файл окажется вредоносным приложением, его сигнатура будет добавлена в следующую версию базы данных сигнатур вирусов.

Отправка анонимной статистической информации: система своевременного обнаружения ESET Live Grid собирает анонимную информацию о компьютере, связанную с новыми обнаруженными угрозами. Эта информация включает имя вредоносной программы, дату и время ее обнаружения, версию приложения ESET, версию операционной системы компьютера и информацию о его расположении. Обычно статистика отправляется на серверы ESET один или два раза в день.

Пример отправляемого пакета со статистикой:

```
# utc_time=2005-04-14 07:21:28
# country="Slovakia"
# language="ENGLISH"
# osver=9.5.0
# engine=5417
# components=2.50.2
# moduleid=0x4e4f4d41
# filesize=28368
# filename=Users/UserOne/Documents/Incoming/
rdgFR1463[1].zip
```

Фильтр исключения: этот параметр позволяет не отправлять определенные типы файлов. Например, можно исключить файлы, в которых может присутствовать конфиденциальная информация, в частности документы и электронные таблицы. Файлы наиболее распространенных типов (.doc, .rtf и т. п.) исключаются по умолчанию. В список исключений можно добавить и другие типы файлов.

Адрес электронной почты (необязательно): адрес электронной почты будет использован, если для анализа потребуются дополнительные данные. Имейте в виду, что компания ESET не связывается с пользователями без необходимости.

11.4 Карантин

Карантин предназначен в первую очередь для безопасного хранения зараженных файлов. Файлы следует помещать на карантин, если они не могут быть излечены или безопасно удалены, если удалять их не рекомендуется или если приложение ESET Endpoint Security посчитало их зараженными файлами ошибочно.

Поместить на карантин можно любой файл. Рекомендуется помещать на карантин файлы, активность которых является подозрительной и которые, тем не менее, модуль сканирования не определяет как зараженные. Файлы на карантине можно отправить на анализ в лабораторию ESET по изучению угроз.

Информацию о файлах в папке карантина можно просмотреть в виде таблицы, содержащей дату и время помещения файла на карантин, путь к его исходному расположению, его размер в байтах, причину помещения на карантин (например, файл был добавлен пользователем) и количество обнаруженных угроз. Папка карантина (*/Library/Application Support/Eset/esets/cache/quarantine*) остается на компьютере даже после удаления программы ESET Endpoint Security. В папке карантина файлы хранятся в безопасном зашифрованном виде. Их можно восстановить после повторной установки приложения ESET Endpoint Security.

11.4.1 Помещение файлов на карантин

Программа ESET Endpoint Security автоматически помещает удаленные файлы на карантин (если пользователь не отключил эту функцию в окне предупреждения). Чтобы вручную поместить файл на карантин, в окне карантина щелкните элемент «Поместить на карантин». Кроме того, чтобы поместить файл в папку карантина, можно щелкнуть файл, удерживая нажатой клавишу CTRL, и в контекстном меню последовательно выбрать пункты «Службы» > «ESET Endpoint Security — добавление файлов в карантин».

11.4.2 Восстановление файла из карантина

Файл, помещенный в карантин, можно восстановить в исходное расположение. Для этого выберите файл и нажмите кнопку **Восстановить**. Восстановить файл можно также с помощью контекстного меню. Удерживая клавишу CTRL, щелкните файл в карантине и выберите пункт **Восстановить**. Чтобы восстановить файл в расположение, отличное от того, в котором он изначально находился, используйте команду **Восстановить в**.

11.4.3 Отправка файла из карантина

Если вы поместили на карантин файл, который программа не обнаружила, или если файл неверно был квалифицирован как зараженный (например, в результате ошибки эвристического метода) и помещен на карантин, отправьте этот файл в лабораторию ESET по изучению угроз. Чтобы отправить файл из карантина, щелкните его правой кнопкой мыши, удерживая клавишу CTRL, и выберите пункт **Отправить файл на анализ**.

11.5 Права

Настройки ESET Endpoint Security могут иметь большое значение для политики безопасности организации. Несанкционированное изменение параметров может нарушить стабильность работы системы и ослабить ее защиту. Чтобы избежать этого, рекомендуется выбрать пользователей, которым разрешено изменять конфигурацию приложения.

Права пользователей можно настроить в меню **Настройка** > **Задать настройки приложения** > **Пользователь** > **Права**.

Для обеспечения максимальной защиты системы необходимо правильно настроить приложение. Несанкционированное изменение настроек может привести к потере важных данных. Чтобы создать список пользователей с правами, в левой части окна в списке **Пользователи** выберите пользователей и нажмите кнопку **Добавить**. Чтобы удалить пользователя, в правой части окна в списке **Пользователи с правами** выберите имя пользователя и нажмите кнопку **Удалить**. Чтобы отобразить всех пользователей системы, установите флажок **Показывать всех пользователей**.

ПРИМЕЧАНИЕ. Если список пользователей с правами пуст, изменять настройки приложения могут все пользователи системы.

11.6 Режим презентации

Режим презентации — функция, которая уменьшает нагрузку на процессор и не позволяет программе мешать пользователю работать с другими приложениями (блокируются все всплывающие окна). В частности, этот режим можно использовать во время проведения презентаций, когда вмешательство модуля защиты от вирусов является крайне нежелательным. Когда этот режим активирован, все всплывающие окна блокируются, а запланированные задачи не запускаются. Защита системы по-прежнему работает в фоновом режиме, но не требует какого-либо вмешательства со стороны пользователя.

Чтобы активировать режим презентации вручную, щелкните **Настройка** > **Задать настройки приложения** > **Режим презентации** > **Включить режим презентации**.

Установите флажок **В полноэкранном режиме автоматически включать режим презентации**. Теперь режим презентации будет автоматически включаться, когда какое-либо приложение будет запускаться на полный экран. После закрытия приложения режим презентации будет автоматически отключаться. Эта функция особенно полезна при проведении презентаций.

Вы также можете выбрать **Автоматически отключать режим презентации через** для указания времени в минутах, через которое режим презентации будет автоматически отключен.

Включая режим презентации вы подвергаете систему угрозе, поэтому значок состояния защиты ESET Endpoint Security станет оранжевым, чтобы тем самым предупредить вас.

ПРИМЕЧАНИЕ. Если персональный файервол работает в интерактивном режиме и включен режим презентации, возможны проблемы при подключении к Интернету. Это может создать некоторые сложности при работе с приложением, которому требуется подключение к Интернету. Обычно пользователю предлагается подтвердить нужное действие (если не задано никаких правил или исключений для подключения), но в режиме презентации взаимодействие с пользователем невозможно. В качестве решения можно создать правило подключения для каждого приложения, которому такое поведение программы может помешать, или использовать другой режим фильтрации в персональном файерволе. Также следует помнить о том, что в режиме презентации доступ к веб-странице или приложению, которые могут представлять угрозу для безопасности, может быть заблокирован. В случае блокировки никакие уведомления не отображаются, поскольку взаимодействие с пользователем отключено.

11.7 Запущенные процессы

В списке **Запущенные процессы** отображаются запущенные на компьютере процессы. Программа ESET Endpoint Security предоставляет подробную информацию о запущенных процессах, обеспечивая защиту пользователей с помощью технологии ESET Live Grid.

- **Процесс**: имя процесса, запущенного в настоящий момент на компьютере. Для просмотра запущенных на компьютере процессов можно также использовать монитор активности (находится в папке */Applications/Utilities*).
- **Уровень риска**: в большинстве случаев программа ESET Endpoint Security и технология ESET Live Grid присваивают уровни риска объектам (файлам, процессам и т. п.) с помощью ряда эвристических правил, которые проверяют характеристики каждого объекта, а затем оценивают их потенциальную способность к вредоносным действиям. На основании этого эвристического анализа объектам присваивается уровень риска. Известные приложения (помечены зеленым цветом) точно являются чистыми (находятся в белом списке) и поэтому исключаются из сканирования. Это повышает скорость сканирования по требованию и сканирования в режиме реального времени. Если приложение помечено как неизвестное (желтый цвет), оно не обязательно является вредоносным. Обычно это просто новое приложение. Если вы не уверены, опасен тот или иной файл, отправьте его на анализ в лабораторию ESET по изучению угроз. Если файл окажется вредоносным приложением, его сигнатура будет добавлена в следующее обновление.
- **Количество пользователей**: количество пользователей, использующих определенное приложение. Эту информацию собирает технология ESET Live Grid.
- **Время обнаружения**: время, прошедшее с того момента, когда приложение было обнаружено технологией ESET Live Grid.
- **Идентификатор пакета приложения**: имя поставщика или процесса приложения.

Если щелкнуть какой-то процесс, в нижней части окна появится дополнительная информация.

- **Файл**: расположение приложения на компьютере.
- **Размер файла**: физический размер файла на диске.
- **Описание файла**: характеристики файла на основании описания, доступного в операционной системе.

- **Идентификатор пакета приложения**: имя поставщика или процесса приложения.
- **Версия файла**: информация от издателя приложения.
- **Имя программы**: название приложения и/или фирменное наименование.

12. Интерфейс

Параметры конфигурации интерфейса позволяют настроить рабочую среду в соответствии с потребностями пользователя. Эти параметры доступны в главном меню в разделе **Настройка** > **Дополнительные настройки...** > **Интерфейс**.

- Для отображения заставки ESET Endpoint Security при запуске системы установите флажок **Показывать заставку при запуске**.
- С помощью параметра **Поместить приложение на панель Dock** можно разместить значок ESET Endpoint Security на панели Dock в ОС macOS и переключаться между программой ESET Endpoint Security и другими запущенными приложениями с помощью сочетания клавиш *cmd+tab*. Изменения вступают в силу после повторного запуска программы ESET Endpoint Security (обычно после перезагрузки компьютера).
- Параметр **Использовать обычное меню** позволяет использовать определенные сочетания клавиш (см. раздел Сочетания клавиш 11) и отображать элементы обычного меню («Интерфейс», «Настройка» и «Служебные программы») в строке меню macOS (в верхней части экрана).
- Установите флажок **Показывать подсказки**, чтобы при наведении указателя на тот или иной параметр ESET Endpoint Security отображалась соответствующая подсказка.
- Параметр **Показывать скрытые файлы** позволяет просматривать и выбирать скрытые файлы при настройке **объектов сканирования** в рамках **сканирования компьютера**.
- По умолчанию значок ESET Endpoint Security отображается в дополнительных элементах строки меню, которые находятся в правой части строки меню macOS (вверху экрана). Чтобы отключить отображение значка, снимите флажок **Показывать значок в дополнительных элементах строки меню**. Это изменение вступает в силу после перезапуска программы ESET Endpoint Security (обычно после перезагрузки компьютера).

12.1 Предупреждения и уведомления

В разделе **Предупреждения и уведомления** можно настроить то, как программа ESET Endpoint Security обрабатывает системные уведомления и предупреждения об угрозах.

Если снять флажок **Отображать предупреждения**, предупреждения выводиться не будут, поэтому делать это без особых причин не рекомендуется. В большинстве случаев лучше оставить этот параметр без изменений (включен). Расширенные параметры описаны в этой главе 32.

Флажок **Отображать уведомления на рабочем столе** включает показ предупреждений, не требующих вмешательства пользователя, на рабочем столе (по умолчанию в правом верхнем углу экрана). Можно задать длительность отображения уведомления, указав значение параметра **Закрывать окна уведомлений автоматически через** X **секунд** (по умолчанию — 5 секунд).

Начиная с версии ESET Endpoint Security 6.2, можно отключить отображение определенных **состояний защиты** в основном окне программы (окно **Состояние защиты**). Дополнительные сведения см. в статье Состояния защиты 33.

12.1.1 Отображение предупреждений

Программа ESET Endpoint Security отображает различные предупреждения и уведомления, сообщающие о доступности обновлений для программы и операционной системы, отключении тех или иных программных компонентов, удалении журналов и т. п. Каждое из этих уведомлений можно отключить, установив флажок **Больше не показывать это диалоговое окно**.

В списке **Список диалоговых окон** (**Настройка** > **Дополнительные настройки...** > **Предупреждения и уведомления** > **Отображение предупреждений: настройка...**) показаны все диалоговые окна предупреждений, которые отображает программа ESET Endpoint Security. Чтобы включить или отключить определенное уведомление, установите флажок слева от **имени окна**. Кроме того, можно задать **условия отображения**, согласно которым будут отображаться уведомления об обновлениях устройств и ОС.

12.1.2 Состояния защиты

Текущее состояние защиты ESET Endpoint Security можно изменить. Для этого нужно активировать или деактивировать состояния, последовательно щелкнув **Настройка** > **Дополнительные настройки...** > **Предупреждения и уведомления** > **Отображать в окне состояния защиты: настройка**. Состояния разных компонентов программы отображаются или не отображаются (если их скрыть) на основном экране ESET Endpoint Security (окно **Состояние защиты**).

Вы можете скрыть состояние защиты следующих компонентов программы:

- Файервол
- Защита от фишинга
- Защита доступа в Интернет
- Защита почтового клиента
- Режим презентации
- Обновление операционной системы
- Окончание срока действия лицензии
- Требуется перезапуск компьютера

12.2 Контекстное меню

Чтобы сделать некоторые функции ESET Endpoint Security доступными в контекстном меню, щелкните **Настройка** > **Задать настройки приложения** > **Контекстное меню** и установите флажок **Интегрировать с контекстным меню**. Изменения вступят в силу при последующем входе в систему или после перезагрузки компьютера. Команды контекстного меню будут доступны на рабочем столе и в окне **Finder**, если щелкнуть любой файл, удерживая нажатой клавишу CTRL.

13. Обновление

Для обеспечения максимального уровня безопасности необходимо регулярно обновлять ESET Endpoint Security. Модуль обновления поддерживает актуальное состояние программы, загружая последнюю версию базы данных сигнатур вирусов.

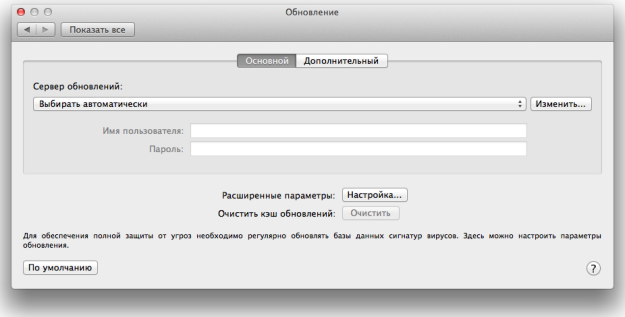
Чтобы просмотреть информацию о текущем состоянии обновления, в том числе дату и время последнего обновления, а также сведения о необходимости обновления, щелкните в главном меню элемент **Обновление**. Чтобы запустить процесс обновления вручную, щелкните **Обновить базу данных сигнатур вирусов**.

Обычно после корректного завершения загрузки в окне обновления выводится сообщение *Обновление не требуется, поскольку установленная база данных сигнатур вирусов является актуальной*. Если обновить базу данных сигнатур вирусов не удается, рекомендуется проверить настройки обновления 33. Самая распространенная причина такой ошибки — неверно введенные данные лицензии 9 или неправильные параметры подключения 36.

В окне **Обновление** также указывается версия базы данных сигнатур вирусов. Номер версии является активной ссылкой на веб-сайт ESET, на котором можно просмотреть все сигнатуры вирусов, включенные в текущее обновление.

13.1 Настройка обновлений

Раздел параметров обновлений содержит информацию об источниках обновлений, такую как адреса серверов обновлений и данные аутентификации для них. По умолчанию в раскрывающемся списке **Сервер обновлений** выбран параметр **Выбирать автоматически**. Благодаря этому файлы обновлений будут загружаться с сервера ESET автоматически и с минимальным расходом трафика.



Доступные серверы обновлений можно просмотреть в раскрывающемся списке **Сервер обновлений**. Чтобы добавить новый сервер, нажмите кнопку **Изменить**, в поле **Сервер обновлений** введите адрес нового сервера и нажмите кнопку **Добавить**.

В ESET Endpoint Security можно настроить альтернативный (резервный) сервер обновлений. Например, **основным сервером** может быть сервер зеркала, а **дополнительным** — стандартный сервер обновлений ESET. Дополнительный сервер должен отличаться от основного, в противном случае он не будет использоваться. Не указав дополнительный сервер обновлений, имя пользователя и пароль, вы не сможете использовать резервный сервер для обновления продукта. Если выбрать значение «Выбирать автоматически» и указать в соответствующих полях имя пользователя и пароль, программа ESET Endpoint Security будет автоматически выбирать наиболее подходящий сервер обновлений.

Режим прокси-сервера позволяет обновлять базу данных сигнатур вирусов через прокси-сервер (например, локальный прокси-сервер HTTP). Это может быть глобальный прокси-сервер, который используют все компоненты программы, требующие подключения, или другой прокси-сервер. Параметры глобального прокси-сервера должны быть заданы при установке или в разделе Настройка прокси-сервера 36.

Чтобы клиент только загружал обновления с прокси-сервера, выполните следующие действия:

1. в раскрывающемся меню выберите **Подключение через прокси-сервер**;
2. щелкните **Обнаружить**, чтобы программа сама ввела IP-адрес и номер порта (**3128** — это номер, используемый по умолчанию);
3. если для соединения с прокси-сервером требуется аутентификация, в соответствующих полях введите правильные **имя пользователя** и **пароль**.

Программа ESET Endpoint Security обнаруживает параметры прокси-сервера, заданные в разделе системных настроек macOS. Их можно настроить в macOS, последовательно щелкнув > **Системные настройки** > **Сеть** > **Дополнительно** > **Прокси-серверы**.

Если установить флажок **Использовать прямое подключение, если прокси-сервер HTTP недоступен** , программа ESET Endpoint Security будет автоматически пытаться подключиться к серверам обновления без использования прокси-сервера. Этот параметр рекомендуется использовать мобильным пользователям, которые используют ноутбуки MacBook.

Если во время загрузки обновлений базы данных сигнатур вирусов возникли осложнения, щелкните **Очистить кэш обновлений**, чтобы удалить временные файлы обновлений.

13.1.1 Расширенные параметры

Чтобы отключить показ оповещений после каждого обновления, установите флажок **Не отображать уведомления об успешном обновлении**.

Включение тестовых обновлений позволит загружать модули, которые находятся на завершающем этапе тестирования. Тестовые обновления зачастую содержат исправления ошибок, которые происходят в работе программы. Загрузка отложенных обновлений выполняется через несколько часов после выпуска — это позволяет убедиться в отсутствии каких-либо ошибок до того, как ваши клиенты получат обновления.

Программа ESET Endpoint Security создает снимки базы данных сигнатур вирусов и модулей программы. Эти снимки используются функцией **Откат обновления**. Установленный флажок **Создавать снимки файлов обновлений** позволит программе ESET Endpoint Security создавать эти снимки автоматически. Если вы подозреваете, что последнее обновление базы данных сигнатур вирусов и/или модулей программы повреждено или работает нестабильно, вы сможете выполнить откат к предыдущей версии и отключить обновления на установленный период времени. Или же можно включить ранее отключенные обновления, если они отложены на неопределенный период времени. При откате к предыдущему обновлению укажите в раскрывающемся списке «Установить такой период приостановки» время, на которое требуется приостановить загрузку обновлений. Если вы выберете вариант «До отзыва», обычные обновления можно будет возобновить только вручную. Используйте этот параметр с осторожностью.

Автоматически задавать максимальный возраст базы данных: с помощью этого параметра можно задать максимальное время (в днях), по истечении которого база данных сигнатур вирусов будет считаться устаревшей. По умолчанию установлено значение «7 дней».

13.2 Создание задач обновления

Чтобы запустить обновление вирусных сигнатур вручную, щелкните «Обновление» > **Обновить базу данных сигнатур вирусов**.

Обновление также можно выполнять по расписанию. Чтобы создать запланированную задачу обновления, перейдите в раздел **Служебные программы** > **Планировщик**. По умолчанию в ESET Endpoint Security активированы следующие задачи:

- **Регулярное автоматическое обновление;**
- **Автоматическое обновление после входа пользователя в систему.**

Каждую из этих задач можно изменить в соответствии с конкретными потребностями. В дополнение к задачам по умолчанию можно создать дополнительные задачи обновления с пользовательскими настройками. Дополнительные сведения о создании и настройке задач обновления см. в разделе Планировщик 27.

13.3 Обновление до новой сборки

Для обеспечения максимальной защиты важно использовать новейшую сборку ESET Endpoint Security. Чтобы проверить наличие новой версии, в главном меню в левой части окна щелкните элемент **Обновление**. Если доступна новая сборка, в нижней части окна отобразится соответствующее уведомление. Щелкните **Подробнее**, чтобы просмотреть номер версии новой сборки и перечень изменений.

Если нажать кнопку **Загрузить**, файл будет загружен в папку загрузок (или в выбранную в браузере папку по умолчанию). Когда файл будет загружен, запустите его и следуйте указаниям по установке. Сведения о вашей лицензии будут автоматически перенесены в новую версию.

Рекомендуется регулярно проверять наличие обновлений, особенно при выполнении установки ESET Endpoint Security с компакт- или DVD-диска.

13.4 Обновления системы

Функция обновления системы macOS является важным компонентом, предназначенным для защиты пользователей от вредоносных программ. В целях обеспечения максимальной безопасности рекомендуется устанавливать эти обновления сразу же после их появления. Программа ESET Endpoint Security будет показывать уведомления о неустановленных обновлениях в соответствии с уровнем важности. Уровень важности обновлений, для которых будут показываться уведомления, можно настроить в меню **Настройка** > **Задать настройки приложения** > **Предупреждения и уведомления > Настройка** (в раскрывающемся списке **Условия отображения** выберите пункт **Обновления операционной системы**.

- **Показывать все обновления**: уведомления будут отображаться для всех неустановленных обновлений.
- **Показывать только рекомендуемые**: уведомления будут отображаться только для рекомендуемых обновлений.

Если вы не хотите получать оповещения о неустановленных обновлениях, снимите флажок **Обновления операционной системы**.

В окне уведомления отображаются общие сведения о доступных обновлениях для операционной системы macOS и приложений, которые обновляются с помощью встроенной в macOS функции обновления программного обеспечения. Чтобы запустить обновление, щелкните в окне уведомления или на **домашней странице** программы ESET Endpoint Security элемент **Установите недостающие обновления**.

В окне уведомления отображается название приложения, его версия, размер, свойства (флаги) и дополнительные сведения о доступных обновлениях. В столбце **Флаги** указана следующая информация:

- **[рекомендуется]**: производитель операционной системы рекомендует установить данное обновление, чтобы повысить уровень безопасности и стабильности системы;
- **[перезагрузка]**: после установки обновления необходимо перезагрузить компьютер;
- **[выключение]**: после установки обновления требуется завершить работу компьютера, а затем снова включить его.

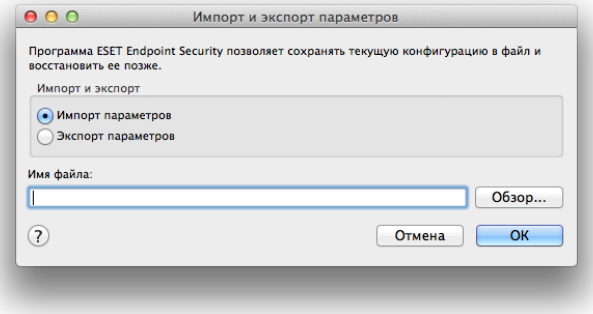
В окне уведомления отображаются обновления, полученные с помощью инструмента командной строки softwareupdate. Полученные таким образом обновления могут отличаться от обновлений, отображаемых в приложении для обновления программного обеспечения. Чтобы установить все доступные обновления, показанные в окне неустановленных обновлений системы, а также те обновления, которые не показаны в приложении для обновления программного обеспечения, используйте инструмент командной строки softwareupdate. Чтобы получить дополнительные сведения об инструменте softwareupdate, введите в окне **Терминал** команду `man softwareupdate`. Использовать инструмент рекомендуется только опытным пользователям.

14. Разное

14.1 Импорт и экспорт параметров

Чтобы импортировать существующую конфигурацию или экспортировать конфигурацию ESET Endpoint Security, последовательно щелкните элементы **Настройка** > **Импорт и экспорт параметров**.

Импорт и экспорт удобно использовать, когда нужно создать резервную копию текущей конфигурации ESET Endpoint Security для дальнейшего использования. Экспорт параметров также можно использовать для переноса желаемой конфигурации ESET Endpoint Security в другие системы — файл конфигурации в считанные секунды импортируется на целевом компьютере.



Чтобы импортировать конфигурацию, выберите **Импортировать параметры** и щелкните **Обзор**, чтобы перейти к файлу конфигурации, который нужно импортировать. Чтобы экспортировать ее, выберите **Экспортировать параметры** и с помощью средства обзора выберите расположение на компьютере, в которое нужно сохранить файл конфигурации.

14.2 Настройка прокси-сервера

Чтобы настроить параметры прокси-сервера, последовательно щелкните элементы **Настройка** > **Дополнительные настройки** > **Прокси-сервер**. Настройка прокси-сервера на этом уровне предусматривает изменение глобальных параметров для всех функций программы ESET Endpoint Security. Они используются всеми модулями, которым требуется подключение к Интернету. Программа ESET Endpoint Security поддерживает следующие типы аутентификации: Basic Access и NTLM (NT LAN Manager).

Чтобы задать параметры прокси-сервера на этом уровне, установите флажок **Использовать прокси-сервер**, а затем введите IP- или URL-адрес прокси-сервера в поле **Прокси-сервер**. В поле «Порт» укажите порт, по которому прокси-сервер принимает запросы на соединение (3128 — это порт, используемый по умолчанию). Кроме того, вы можете щелкнуть **Обнаружить**, чтобы программа заполнила оба поля.

Если для соединения с прокси-сервером требуется аутентификация, в соответствующих полях введите правильные **имя пользователя** и **пароль**.

14.3 Общий локальный кэш

Чтобы активировать использование общего локального кэша, последовательно щелкните «Настройка» > «Задать настройки приложения» > «Общий локальный кэш» и установите флажок «Включить кэширование с использованием общего локального кэша ESET». Эта функция повышает производительность в виртуализированных средах, предотвращая повторное сканирование объектов в сети: каждый файл сканируется только один раз, а затем сохраняется в общий кэш. Когда функция активирована, сведения о сканировании файлов и папок в сети сохраняется в локальный кэш. При следующем сканировании продукт ESET Endpoint Security будет искать сканируемые файлы в кэше и в случае обнаружения будет исключать их из сканирования.

Доступны следующие настройки общего локального кэша:

- **Имя хоста**: имя или IP-адрес компьютера, на котором расположен кэш;
- **Порт**: номер порта, используемого для подключения (3537 — это номер, используемый по умолчанию);
- **Пароль**: пароль общего локального кэша (необязательный параметр).

ПРИМЕЧАНИЕ. Подробные инструкции по установке и настройке общего локального кэша ESET см. в руководстве пользователя по общему локальному кэшу ESET. (Данное руководство доступно только на английском языке.)