ESET Endpoint Security for macOS

Руководство пользователя

Щелкните здесь чтобы отобразить этого документа (онлайн-справка)

Digital Security
Progress. Protected.

ESET Endpoint Security for macOS разработано компанией ESET, spol. s r.o.

Дополнительные сведения можно получить на сайте https://www.eset.com.

Служба технической поддержки: https://support.eset.com

ПРОВ. 19.03.2023

ESET Endpoint Security for macOS

Программа ESET Endpoint Security for macOS 6 представляет собой новый подход к созданию действительно комплексной системы безопасности компьютера. Актуальная версия модуля сканирования ThreatSense®в сочетании с нашим специализированным 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 for macOS 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.

Этот продукт предназначен в первую очередь для использования на рабочих станциях в средах небольших и крупных предприятий. Его можно использовать с ESET PROTECT (ранее ESET Security Management Center), что позволяет с легкостью управлять любым количеством клиентских рабочих станций, применять политики и правила, отслеживать обнаружения и удаленно вносить изменения с любого подключенного к сети компьютера.

Новые возможности в версии 6

Графический интерфейс пользователя ESET Endpoint Security for macOS полностью изменен: внешний вид стал лучше, а работа с приложением — более интуитивно понятной. Ниже приведены некоторые улучшения в версии 6 приложения.

- Поддержка ESET Enterprise Inspector: начиная с версии 6.9 решение ESET Endpoint Security for macOS можно соединить с ESET Enterprise Inspector. ESET Enterprise Inspector (EEI) — это комплексная система обнаружения и реагирования для конечных точек, которая включает в себя такие функции, как обнаружение инцидентов, управление инцидентами и реагирование на них, сбор данных, индикаторы обнаружения взлома, обнаружение аномалий, обнаружение поведения, нарушения политики. Для получения дополнительных сведений о решении ESET Enterprise Inspector, его установке и функциях воспользуйтесь справкой по ESET Enterprise Inspector.

- **Поддержка 64-разрядной архитектуры**

- **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 неприемлемые или оскорбительные материалы.

- **Защита доступа в Интернет**: отслеживает обмен данными между веб-браузерами и

удаленными серверами.

- **Защита электронной почты**: позволяет контролировать обмен почтовыми сообщениями через протоколы 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 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 for macOS работать в фоновом режиме и блокирует все всплывающие окна и запланированные задачи.

- **Общий локальный кэш**: повышает скорость сканирования в виртуализированных средах.

Требования к системе

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

	Системные требования:
Архитектура процессора	Intel 64-bit, Apple ARM 64-разрядный
Операционная система	macOS 10.12 и более поздние версии
Память	300 МБ
Объем свободного места на диске	200 МБ

В дополнение к существующей поддержке Intel ESET Endpoint Security for macOS 6.10.900.0 и более поздние версии поддерживают процессор Apple ARM с использованием Rosetta 2.

Знакомство с ESET PROTECT

ESET PROTECT дает возможность управлять продуктами ESET на рабочих станциях, серверах и мобильных устройствах в сетевой среде из одного центрального местоположения.

С помощью веб-консоли ESET PROTECT можно развертывать решения ESET, управлять задачами, применять политики безопасности, отслеживать состояние системы и оперативно реагировать на проблемы и обнаружения, возникающие на удаленных компьютерах. Ознакомьтесь также с разделами Обзор архитектуры и элементов инфраструктуры ESET PROTECT, Начало работы с веб-консолью ESET PROTECT и Поддерживаемые среды подготовки рабочих столов.

ESET PROTECT состоит из следующих компонентов.

• Сервер ESET PROTECT. Сервер ESET PROTECT устанавливается на сервера под управлением Windows или Linux, а также в качестве виртуального устройства. Он управляет связью с агентами, собирает и сохраняет данные приложений в базе данных.

• Веб-консоль ESET PROTECT. Веб-консоль ESET PROTECT является основным интерфейсом, который позволяет управлять клиентскими компьютерами в вашей среде. В ней отображаются общие сведения о состоянии клиентов в сети, и ее можно использовать для удаленного развертывания решений ESET на неуправляемых компьютерах. После установки сервера ESET PROTECT (сервера) вы можете получить доступ к веб-консоли с помощью браузера. Если разрешить доступ к веб-серверу из Интернета, можно будет использовать ESET PROTECT практически в любом месте и на любом устройстве с подключением к Интернету.

• ESET Management Агент. Агент ESET Management облегчает обмен данными между сервером ESET PROTECT и клиентскими компьютерами. Агент должен быть установлен на клиентском компьютере, чтобы установить связь между этим компьютером и сервером ESET PROTECT. Поскольку он находится на клиентском компьютере и может хранить несколько сценариев безопасности, использование ESET Management значительно сокращает время реагирования на новые обнаружения. С помощью веб-консоли ESET PROTECT можно развернуть агент ESET Management на неуправляемых компьютерах, распознанных с помощью Active Directory или ESET RD Sensor. Можно также вручную установить агент ESET Management на клиентских компьютерах, если это необходимо.

• Rogue Detection Sensor. ESET PROTECT Rogue Detection (RD) Sensor обнаруживает неуправляемые компьютеры, присутствующие в сети, и отправляет сведения о них на сервер ESET PROTECT. Это позволяет легко добавлять новые клиентские компьютеры в защищенную сеть. Rogue Detection Sensor запоминает компьютеры, которые были обнаружены, и не будет отправлять одну и ту же информацию дважды.

• Прокси-сервер Apache HTTP. Это служба, которую можно использовать вместе с ESET PROTECT, чтобы:

  оРассылать обновления на клиентские компьютеры и установочные пакеты — агенту ESET Management.

  оПересылать данные с агентов ESET Management на сервер ESET PROTECT.

• Средство подключения для мобильных устройств — это компонент, позволяющий использовать средства управления мобильными устройствами в ESET PROTECT для управления мобильными устройствами (Android и iOS) и администрирования ESET Endpoint Security для Android.

• Виртуальное устройство ESET PROTECT — виртуальное устройство ESET PROTECT доступно для пользователей, которым требуется запустить ESET PROTECT в виртуализированной среде.

• Хост виртуального агента ESET PROTECT — компонент ESET PROTECT, который виртуализирует сущности агентов, позволяя управлять безагентными виртуальными машинами. Это решение обеспечивает автоматизацию, использование динамических групп и тот же уровень управления задачами, что и агент ESET Management на физических компьютерах. Виртуальный агент собирает информацию с виртуальных машин и передает ее на сервер ESET PROTECT.

• Средство «Зеркало». Это средство необходимо для автономного обновления модулей. Если

у клиентских компьютеров нет подключения к Интернету и при этом им нужны обновления модулей, с помощью средства «Зеркало» можно загрузить файлы обновления с серверов обновления ESET и хранить эти файлы локально.

- ESET Remote Deployment Tool. Этот инструмент предназначен для развертывания комплексных пакетов, созданных в веб-консоли <%PRODUCT%>. Это удобный способ распространения агентов ESET Management с продуктом ESET на компьютерах по сети.

- ESET Business Account. Новый портал лицензирования для бизнес-продуктов ESET позволяет управлять своими лицензиями. См. раздел ESET Business Account этого документа, чтобы узнать больше об активации своего продукта, или см. ESET Business Account руководство пользователя, чтобы получить дополнительные сведения об использовании ESET Business Account. Если у вас уже есть имя пользователя и пароль, предоставленные компанией ESET и которые нужно преобразовать в лицензионный ключ, см. раздел Преобразование учетных данных устаревшей лицензии.

- ESET Enterprise Inspector (EEI) — это комплексная система обнаружения и реагирования конечных точек, которая включает в себя такие функции, как обнаружение инцидентов, управление инцидентами и реагированием, сбор данных, индикаторы обнаружения компромиссов, обнаружение аномалий, обнаружение поведения, нарушения политики.

С помощью веб-консоли ESET PROTECT можно развертывать решения ESET, управлять задачами, применять политики безопасности, отслеживать состояние системы и оперативно реагировать на проблемы и угрозы, возникающие на удаленных компьютерах.

ℹ Дополнительные сведения см. в интерактивном руководстве пользователя ESET PROTECT.

Знакомство с ESET PROTECT CLOUD

ESET PROTECT CLOUD дает возможность управлять продуктами ESET на рабочих станциях и серверах в сетевой среде из одного центрального местоположения без необходимости использовать физический или виртуальный сервер, как в случае с ESET PROTECT или ESET Security Management Center. С помощью веб-консоли ESET PROTECT CLOUD можно развертывать решения ESET, управлять задачами, применять политики безопасности, отслеживать состояние системы и оперативно реагировать на проблемы и угрозы, возникающие на удаленных компьютерах.

- Дополнительные сведения см. в интерактивном руководстве пользователя ESET PROTECT CLOUD

Удаленная установка

Перед установкой

macOS 10.15 и более ранние версии

Перед установкой ESET Endpoint Security for macOS в системе macOS 10.13 и более поздних версиях разрешите расширения ядра ESET, а в системе macOS 10.14 и более поздних версиях также разрешите полный доступ к диску на целевых компьютерах. Если после установки эти

параметры разрешены, пользователи будут получать уведомления **Расширения системы заблокированы** и **Ваш компьютер защищен частично**, пока не будут разрешены расширения ядра ESET и полный доступ к диску.

Чтобы удаленно разрешить расширения ядра ESET и полный доступ к диску, ваш компьютер должен быть зарегистрирован на сервере MDM (Mobile Device Management — управления мобильными устройствами), например Jamf.

Разрешение расширений системы ESET

Чтобы удаленно разрешить расширения ядра на вашем устройстве, выполните следующие действия.

- Если вы используете Jamf как сервер MDM, следуйте указаниям в статье нашей базы знаний.

- Если вы используете другой сервер MDM, загрузите профиль конфигурации с расширением .plist. Воспользовавшись предпочитаемым генератором UUID, создайте два UUID-идентификатора и с помощью текстового редактора замените в загруженном профиле конфигурации строки с текстом `insert your UUID 1 here` (Вставьте идентификатор UUID 1 здесь) и `insert your UUID 2 here` (Вставьте идентификатор UUID 2 здесь). Разверните файл профиля конфигурации с расширением .plist с помощью сервера MDM. Чтобы на компьютере можно было развертывать профили конфигурации, такой компьютер должен быть зарегистрирован на сервере MDM.

Разрешение полного доступа к диску

В системе macOS 10.14 вы получите уведомление от программы ESET Endpoint Security for macOS после ее установки о том, что **ваш компьютер защищен частично**. Чтобы получить доступ ко всем функциям ESET Endpoint Security for macOS и не получать больше это уведомление, необходимо разрешить программе ESET Endpoint Security for macOS **полный доступ к диску** перед установкой этого продукта. Чтобы удаленно разрешить **полный доступ к диску**, выполните следующие действия.

- Если вы используете Jamf как сервер MDM, следуйте указаниям в статье нашей базы знаний.

- Чтобы удаленно разрешить **полный доступ к диску**, загрузите файл конфигурации с расширением .plist. Воспользовавшись предпочитаемым генератором UUID, создайте два UUID-идентификатора и с помощью текстового редактора замените в загруженном профиле конфигурации строки с текстом `insert your UUID 1 here` (Вставьте идентификатор UUID 1 здесь) и `insert your UUID 2 here` (Вставьте идентификатор UUID 2 здесь). Разверните файл профиля конфигурации с расширением .plist с помощью сервера MDM. Чтобы иметь возможность разворачивать профили конфигурации на компьютере, он должен быть зарегистрирован на сервере MDM.

macOS Big Sur (11)

Перед установкой ESET Endpoint Security for macOS в системе macOS Big Sur разрешите расширения системы ESET и полный доступ к диску на целевых компьютерах. Если после установки эти параметры разрешены, пользователи будут получать уведомления **Расширения системы**

заблокированы и **Ваш компьютер защищен частично**, пока не будут разрешены расширения системы ESET и полный доступ к диску. Расширения системы можно разрешить удаленно только перед установкой ESET Endpoint Security for macOS.

Чтобы удаленно разрешить расширения системы ESET и полный доступ к диску, ваш компьютер должен быть зарегистрирован на сервере MDM (Mobile Device Management — управления мобильными устройствами), например Jamf.

Разрешение расширений системы ESET

Чтобы удаленно разрешить расширения системы на вашем устройстве, выполните следующие действия.

- Если вы используете Jamf как сервер MDM, следуйте указаниям в статье нашей базы знаний.

- Если вы используете другой сервер MDM, загрузите профиль конфигурации с расширением .plist. Разверните файл профиля конфигурации с расширением .plist с помощью сервера MDM. Чтобы на компьютере можно было развертывать профили конфигурации, такой компьютер должен быть зарегистрирован на сервере MDM. Чтобы создать собственный профиль конфигурации, используйте следующие настройки:

Идентификатор команды (TeamID)	`P8DQRXPVLP`

Идентификатор пакета (BundleID)	`com.eset.endpoint`
	`com.eset.network`
	`com.eset.firewall`
	`com.eset.devices`

Разрешение полного доступа к диску

Чтобы удаленно разрешить **полный доступ к диску**, выполните следующие действия.

- Если вы используете Jamf как сервер MDM, следуйте указаниям в статье нашей базы знаний.

- Чтобы удаленно разрешить **полный доступ к диску**, загрузите файл конфигурации с расширением .plist. Разверните файл профиля конфигурации с расширением .plist с помощью сервера MDM. Чтобы на компьютере можно было развертывать профили конфигурации, такой компьютер должен быть зарегистрирован на сервере MDM. Чтобы создать собственный профиль конфигурации, используйте следующие настройки:

ESET Endpoint Security	
Идентификатор	`com.eset.ees.6`
Тип идентификатора	`bundleID`
Требование к коду	`identifier "com.eset.ees.6" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = P8DQRXPVLP`
Приложение или служба	`SystemPolicyAllFiles`
Доступ	`Allow`

ESET Endpoint Antivirus и ESET Endpoint Security	
Идентификатор	`com.eset.devices`
Тип идентификатора	`bundleID`
Требование к коду	`identifier "com.eset.devices" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = P8DQRXPVLP`
Приложение или служба	`SystemPolicyAllFiles`
Доступ	`Allow`

ESET Endpoint Antivirus и ESET Endpoint Security	
Идентификатор	`com.eset.endpoint`
Тип идентификатора	`bundleID`
Требование к коду	`identifier "com.eset.endpoint" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = P8DQRXPVLP`
Приложение или служба	`SystemPolicyAllFiles`
Доступ	`Allow`

Установка

Перед установкой вы можете создать пакет для удаленной установки с предварительно заданной конфигурацией ESET Endpoint Security for macOS, который можно затем развернуть с помощью ESET PROTECT или MDM по вашему выбору.

- Создайте пакет для удаленной установки.

Установите ESET Endpoint Security for macOS удаленно, создав **задачу «Установка программного обеспечения»** с помощью системы управления ESET:

- Задача установки программного обеспечения ESET PROTECT
- Задача установки программного обеспечения ESET Security Management Center

После установки

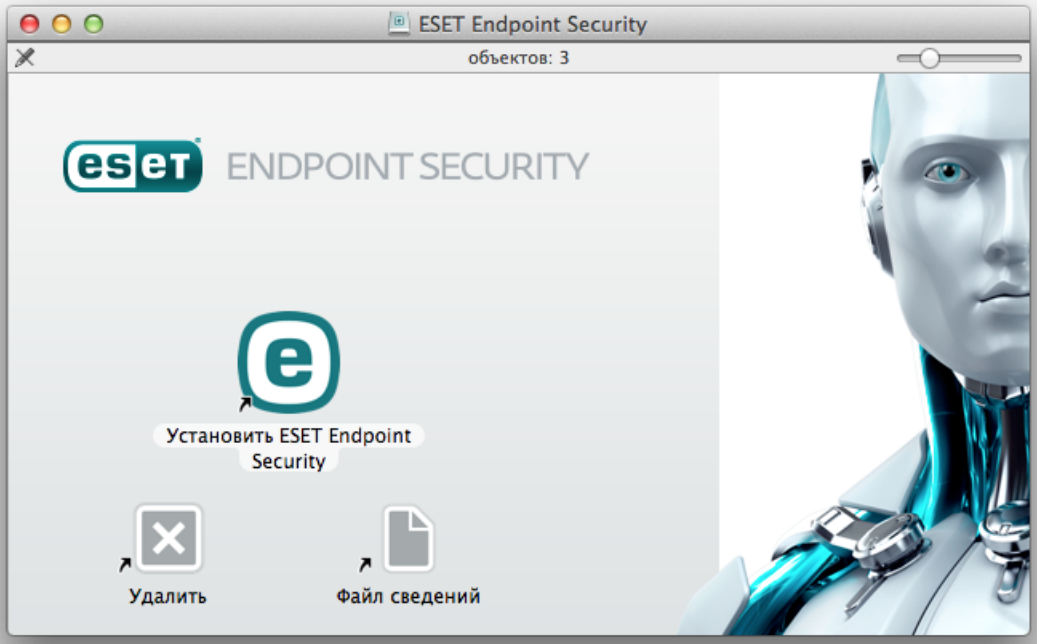
Пользователи получат следующее уведомление: ESET Endpoint Security for macOS **хочет фильтровать сетевое содержимое**. Получив это уведомление, пользователям следует щелкнуть **Разрешить**. Если щелкнуть **Не разрешать**, защита доступа в Интернет работать не будет.

Создание пакета для удаленной установки

Создание пакета для установки Apple Remote Desktop

1. Загрузите стандартный пакет для установки с веб-сайта ESET:
ESET Endpoint Security for macOS

2. Чтобы запустить установщик ESET Endpoint Security for macOS, дважды щелкните загруженный файл.



1. Щелкните **Установить**ESET Endpoint Security for macOS.

2. При появлении соответствующего запроса щелкните **Разрешить**, чтобы установщик мог определять, можно ли устанавливать программное обеспечение.

3. Щелкните **Продолжить**. Если вы создаете пакет для удаленной установки, решение ESET Endpoint Security for macOS установлено не будет.

4. Просмотрите системные требования и щелкните **Продолжить**.

5. Прочтите лицензионное соглашение на использование программного обеспечения ESET и щелкните **Продолжить** → **Я принимаю**, если вы принимаете условия.

6. На этапе **Режим установки** выберите **Удаленная**.

7. Выберите, какие компоненты продукта нужно установить. По умолчанию выбраны все компоненты. Щелкните **Продолжить**.

8. На этапе **Прокси-сервер** выберите параметр, который соответствует вашему

подключению к Интернету. Если вы не уверены, используйте системные настройки по умолчанию. Щелкните **Далее**. Если вы используете прокси-сервер, на следующем этапе вам будет предложено ввести адрес прокси-сервера, имя пользователя и пароль.

9. Выберите, кто может изменять конфигурацию программы. Изменить ее могут только привилегированные пользователи и группы. По умолчанию группа администраторов выбрана в качестве привилегированной. Установите флажок **Показывать всех пользователей** или **Показывать все группы**, чтобы отобразить всех виртуальных пользователей и все группы, например программы и процессы.

10. При необходимости включите ESET LiveGrid на целевом компьютере.

11. При необходимости включите обнаружение потенциально нежелательных приложений на целевом компьютере.

12. Выберите режим файервола:
Автоматический режим: 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 правила, определенные пользователем.

Интерактивный режим: позволяет создать собственную конфигурацию 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 новое правило для файервола. После создания нового правила все будущие подключения этого типа будут разрешены или запрещены в зависимости от параметров правила.

13. Сохраните установочный файл на компьютере. Если вы ранее создавали установочный файл в расположении по умолчанию, прежде чем продолжить, измените расположение папки назначения или удалите предыдущие файлы. Таким образом завершается первая фаза удаленной установки. Происходит выход из локального установщика и в выбранной вами папке назначения создаются файлы для удаленной установки.

Ниже перечислены файлы для удаленной установки.

- *esets_setup.dat*: данные настройки, которые вы ввели в разделе «Настройка» установщика.

- *program_components.dat*: сведения о настройке выбранных компонентов программы. (Этот файл необязателен. Он создается, если вы решили не устанавливать определенные компоненты ESET Endpoint Security for macOS.)

- *esets_remote_install.pkg*: пакет для удаленной установки.

- *esets_remote_uninstall.sh*: сценарий для удаленного удаления.

Установка Apple Remote Desktop

1. Откройте Apple Remote Desktop и подключитесь к целевому компьютеру. Дополнительные сведения можно найти в документации по Apple Remote Desktop.

2. Воспользовавшись функцией **копирования файлов или папок** в Apple Remote Desktop, скопируйте следующие файлы в папку */tmp* на целевом компьютере.

Если вы устанавливаете все компоненты, скопируйте:
- *esets_setup.dat*.

Если вы устанавливаете не все компоненты продукта, скопируйте:
- *esets_setup.dat*,
- *product_components.dat*.

3. Используйте команду **Установить пакеты**, чтобы установить *esets_remote_install.pkg* на целевой компьютер.

Удаленное удаление Apple Remote Desktop

1. Откройте Apple Remote Desktop и подключитесь к целевому компьютеру. Дополнительные сведения можно найти в документации по Apple Remote Desktop.

2. Воспользовавшись функцией **копирования файлов или папок** в Apple Remote Desktop, скопируйте сценарий *esets_remote_uninstall.sh* в папку */tmp* на целевом компьютере.

3. В Apple Remote Desktop примените следующую **команду «Отправить оболочку UNIX»** к целевому компьютеру:

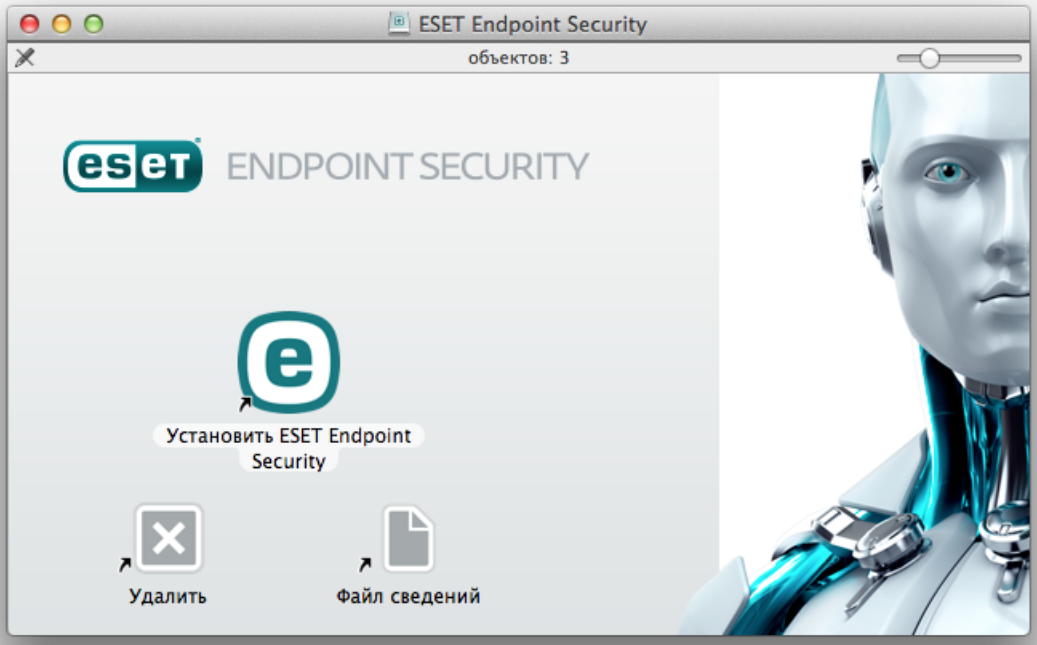
```
/tmp/esets_remote_uninstall.sh
```

По завершении удаления в Apple Remote Desktop на целевом компьютере отобразится консоль.

Установка

Мастер установки поможет настроить основные параметры. Подробное руководство см. в нашей статье базы знаний по установке.

1. Чтобы запустить установщик ESET Endpoint Security for macOS, дважды щелкните загруженный файл.



1. Чтобы начать установку, щелкните **Установить** ESET Endpoint Security for macOS.

Установка с помощью PKG-файла

Ваш компьютер Mac должен быть подключен к Интернету во время установки и запуска продуктов ESET для macOS, чтобы система Apple могла проверить подлинность расширений системы ESET.

2. При появлении соответствующего запроса щелкните **Разрешить**, чтобы установщик мог определять, можно ли устанавливать программное обеспечение.

3. Если вы еще этого не сделали, удалите с компьютера все имеющиеся приложения безопасности, например программы для защиты от вирусов и шпионских программ либо файерволы. Щелкните **Продолжить**, если другие приложения безопасности не установлены.

4. Просмотрите системные требования и щелкните **Продолжить**.

5. Прочтите лицензионное соглашение на использование программного обеспечения ESET и щелкните **Продолжить** → **Я принимаю**, если вы принимаете условия.

6. Выберите подходящий тип установки.

- Обычная установка
- Выборочная установка
- Удаленная установка

> **Обновление версии**
> 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.

Обычная установка

В режиме обычной установки используются параметры конфигурации, 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.

1. В окне **ESET LiveGrid** выберите предпочтительный вариант и щелкните **Продолжить**. Если позже вы решите изменить этот параметр, вы сможете сделать это с помощью **настройки LiveGrid**. Дополнительные сведения о ESET Live Grid приведены в глоссарии.
2. В окне **Потенциально нежелательные приложения** выберите предпочтительный вариант (см. Что собой представляет потенциально нежелательное приложение?) и щелкните **Продолжить**. Если позже вы решите изменить этот параметр, воспользуйтесь **расширенными параметрами**.

3. Щелкните **Установить**. Если вам будет предложено ввести пароль macOS, введите его и щелкните **Установить программное обеспечение**.

После установки ESET Endpoint Security for macOS:

macOS Big Sur (11)

1. Разрешение расширений системы.

2. Разрешение полного доступа к диску.

3. Разрешите ESET добавлять конфигурации прокси-сервера. Вы получите следующее уведомление: ESET Endpoint Security for macOS **хочет фильтровать сетевое содержимое**. Получив это уведомление, щелкните **Разрешить**. Если щелкнуть **Не разрешать**, защита доступа в Интернет работать не будет.

macOS 10.15 и более ранние версии

1. В системе macOS 10.13 и более поздних версиях вы получите системное уведомление о том, что **расширение системы заблокировано**, а ESET Endpoint Security for macOS отобразит уведомление о том, что **компьютер не защищен**. Чтобы получить доступ ко всем функциям ESET Endpoint Security for macOS, необходимо разрешить расширения ядра на вашем устройстве. Для этого последовательно выберите элементы **Системные настройки** > **Безопасность и конфиденциальность** и щелкните **Разрешить**, чтобы разрешить системное программное обеспечение от разработчика **ESET, spol. s.r.o.** Более подробные сведения см. в статье нашей базы знаний.

2. В системе macOS 10.14 и более поздние версии вы получите уведомление программы ESET Endpoint Security for macOS о том, что **ваш компьютер защищен частично**. Чтобы

получить доступ ко всем функциям ESET Endpoint Security for macOS, необходимо разрешить **полный доступ к диску** для программы ESET Endpoint Security for macOS. Щелкните **Открыть параметры системы** > **Безопасность и конфиденциальность**. Перейдите на вкладку **Конфиденциальность** и выберите параметр **Полный доступ к диску**. Щелкните значок замка, чтобы разрешить редактирование. Щелкните значок плюса и выберите приложение ESET Endpoint Security for macOS. На компьютере отобразится уведомление о необходимости перезагрузить систему. Щелкните **Позже**. Пока не перезагружайте компьютер. Щелкните **Начать заново** в окне уведомления программы ESET Endpoint Security for macOS или перезагрузите компьютер. Более подробные сведения см. в статье нашей базы знаний.

После установки ESET Endpoint Security for macOS следует выполнить сканирование компьютера для проверки на наличие вредоносного кода. В главном окне программы выберите пункт **Сканирование компьютера** > **Интеллектуальное сканирование**. Дополнительную информацию о сканировании компьютера по требованию см. в разделе Сканирование компьютера по требованию.

Выборочная установка

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

• **Компоненты программы**
Решение ESET Endpoint Security for macOS 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, установив флажок **Я использую прокси-сервер**, чтобы задать его параметры. В следующем окне введите IP-адрес или URL-адрес прокси-сервера в поле **Адрес**. В поле **Порт** укажите порт, по которому прокси-сервер принимает запросы на соединение (по умолчанию используется порт 3128). 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 **Использовать системные параметры (рекомендуется)**.

• **Разрешения**
Можно определить привилегированных пользователей или группы, которые смогут изменять настройки 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 будут расцениваться как привилегированные.

• **ESET LiveGrid®**
Дополнительные сведения о ESET LiveGrid® приведены в глоссарии.

• **Потенциально нежелательные приложения**
Дополнительные сведения о потенциально нежелательных приложениях приведены в

глоссарии.

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

После установки ESET Endpoint Security for macOS:

macOS Big Sur (11)

1. Разрешение расширений системы.

2. Разрешение полного доступа к диску.

3. Разрешите ESET добавлять конфигурации прокси-сервера. Вы получите следующее уведомление: ESET Endpoint Security for macOS **хочет фильтровать сетевое содержимое**. Получив это уведомление, щелкните **Разрешить**. Если щелкнуть **Не разрешать**, защита доступа в Интернет работать не будет.

macOS 10.15 и более ранние версии

1. В системе macOS 10.13 и более поздних версиях вы получите системное уведомление о том, что **расширение системы заблокировано**, а ESET Endpoint Security for macOS отобразит уведомление о том, что **компьютер не защищен**. Чтобы получить доступ ко всем функциям ESET Endpoint Security for macOS, необходимо разрешить расширения ядра на вашем устройстве. Для этого последовательно выберите элементы **Системные настройки** > **Безопасность и конфиденциальность** и щелкните **Разрешить**, чтобы разрешить системное программное обеспечение от разработчика **ESET, spol. s.r.o.** Более подробные сведения см. в статье нашей базы знаний.

2. В системе macOS 10.14 и более поздние версии вы получите уведомление программы ESET Endpoint Security for macOS о том, что **ваш компьютер защищен частично**. Чтобы получить доступ ко всем функциям ESET Endpoint Security for macOS, необходимо разрешить **полный доступ к диску** для программы ESET Endpoint Security for macOS. Щелкните **Открыть параметры системы** > **Безопасность и конфиденциальность**. Перейдите на вкладку **Конфиденциальность** и выберите параметр **Полный доступ к диску**. Щелкните значок замка, чтобы разрешить редактирование. Щелкните значок плюса и выберите приложение ESET Endpoint Security for macOS. На компьютере отобразится уведомление о необходимости перезагрузить систему. Щелкните **Позже**. Пока не перезагружайте компьютер. Щелкните **Начать заново** в окне уведомления программы ESET Endpoint Security for macOS или перезагрузите компьютер. Более подробные сведения см. в статье нашей базы знаний.

После установки ESET Endpoint Security for macOS выполните сканирование компьютера для проверки на наличие вредоносного кода. В главном окне программы выберите пункт **Сканирование компьютера** > **Интеллектуальное сканирование**. Дополнительную информацию о сканировании компьютера по требованию см. в разделе Сканирование компьютера по требованию.

Разрешение расширений системы на локальном уровне

В macOS 11 (Big Sur) расширения ядра были заменены на расширения системы. Перед загрузкой новых сторонних расширений системы необходимо разрешение пользователя.

После установки ESET Endpoint Security for macOS в системе macOS Big Sur (11) и более поздних версиях вы получите системное уведомление о том, что расширение системы заблокировано, а ESET Endpoint Security for macOS отобразит уведомление о том, что компьютер не защищен. Чтобы получить доступ ко всем функциям ESET Endpoint Security for macOS, необходимо разрешить расширения системы на вашем устройстве.

> **Обновление с предыдущей версии macOS до Big Sur**
> Если вы уже установили ESET Endpoint Security for macOS и собираетесь обновить систему macOS до версии Big Sur, после обновления будет необходимо вручную разрешить расширения ядра ESET. Необходим физический доступ к компьютеру клиента — при удаленном доступе кнопка «Разрешить» отключена.

При установке продукта ESET в системе macOS Big Sur или в более поздних ее версиях необходимо вручную разрешить расширения системы ESET. Необходим физический доступ к компьютеру клиента — при удаленном доступе этот параметр отключен.

Разрешение расширений системы вручную

1. Щелкните **Открыть параметры системы** или **Открыть параметры безопасности** в одном из диалоговых окон с предупреждением.

2. Щелкните значок замка в нижней левой части, чтобы разрешить изменения в окне настроек.

3. Используйте Touch ID или щелкните **Использовать пароль** и введите имя пользователя и пароль, а затем щелкните **Разблокировать**.

4. Щелкните **Подробности**.

5. Выберите все три параметра ESET Endpoint Security for macOS**.app**.

6. Нажмите кнопку **OK**.

Подробное пошаговое руководство см. в статье нашей базы знаний. (Статьи базы знаний доступны не на всех языках.)

Разрешение полного доступа к диску на локальном уровне

В системе macOS 10.14 вы получите уведомление от программы ESET Endpoint Security for macOS о том, что **ваш компьютер защищен частично**. Для доступа ко всем функциям ESET Endpoint Security for macOS необходимо разрешить программе ESET Endpoint Security for macOS **полный**

доступ к диску.

1. Щелкните **Открыть параметры системы** в диалоговом окне предупреждения.

2. Щелкните значок замка в нижней левой части, чтобы разрешить изменения в окне настроек.

3. Используйте Touch ID или щелкните **Использовать пароль** и введите имя пользователя и пароль, а затем щелкните **Разблокировать**.

4. Выберите ESET Endpoint Security for macOS**.app** из списка.

5. Отобразится уведомление о перезапуске ESET Endpoint Security for macOS. Щелкните «Позже».

6. Выберите в списке **Защита файловой системы в реальном времени** ESET.

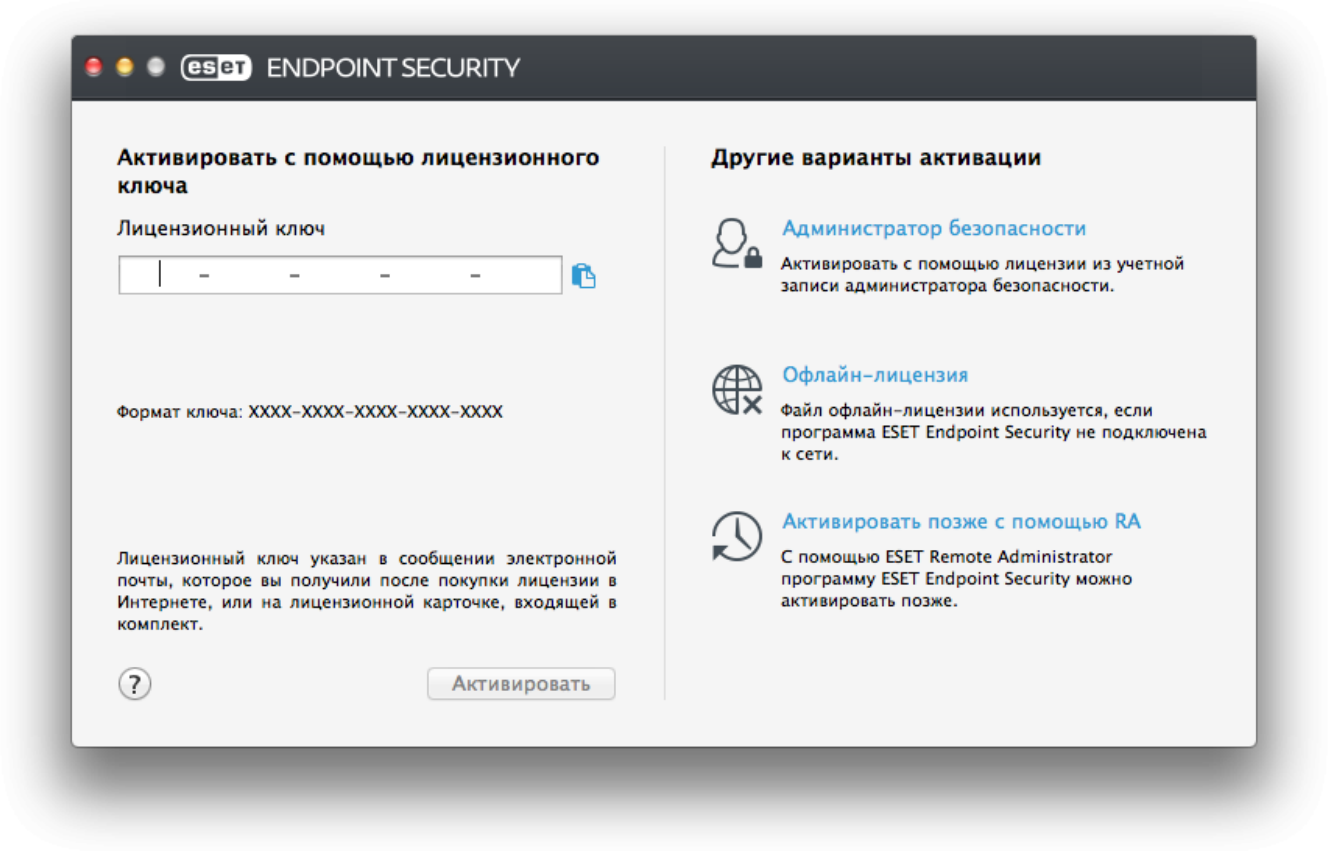
> **Отсутствие защиты файловой системы в реальном времени ESET**
> Если в списке нет опции **Защита файловой системы в реальном времени**, необходимо разрешить расширения системы для продукта ESET.

7. Щелкните «Начать снова» в диалоговом окне предупреждения ESET Endpoint Security for macOS или перезапустите компьютер. Более подробные сведения см. в статье нашей базы знаний.

Активация продукта

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 for macOS непосредственно в приложении, щелкните значок ESET Endpoint Security for macOS, размещенный в строке меню macOS (в верхней части экрана), а затем щелкните элемент **Активация продукта**. 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 for macOS можно воспользоваться любым из перечисленных ниже методов.

- **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.

Автоматическая активация

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

В ESET Endpoint Security for macOS версии 6.3.85.0 (и в более поздних версиях) программу можно

активировать 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 for macOS или зарегистрирован на портале ESET License Administrator. В результате выполнения команды отобразится состояние «OK» или сообщение об ошибке, если активация закончится неудачей.

Удаление

Запустить средство удаления ESET Endpoint Security for macOS можно двумя способами:

- Откройте установочный файл ESET Endpoint Security for macOS (*.dmg*) и дважды щелкните элемент **Удалить**.

- Запустите программу **Finder**, откройте папку **Приложения** на жестком диске, щелкните, удерживая клавишу CTRL, значок **ESET Endpoint Security for macOS**, а затем выберите команду **Показать содержимое пакета**. Откройте папку **Contents** > **Helpers** и дважды щелкните значок **Uninstaller**.

> **Удаление программы**
> В процессе удаления необходимо несколько раз ввести пароль администратора, чтобы полностью удалить программу ESET Endpoint Security for macOS.

Основные сведения

Главное окно ESET Endpoint Security for macOS 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.

- **Обновление**: отображение информации об обновлении модулей.

- **Настройка**: этот раздел используется для настройки уровня безопасности компьютера.

- **Служебные программы**: этот раздел предоставляет доступ к файлам журналов, планировщику, карантину, запущенным процессам и другим возможностям программы.

- **Справка**: обеспечивает доступ к файлам справки, базе знаний в Интернете, форме запроса на получение поддержки и дополнительной информации о программе.

Сочетания клавиш

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

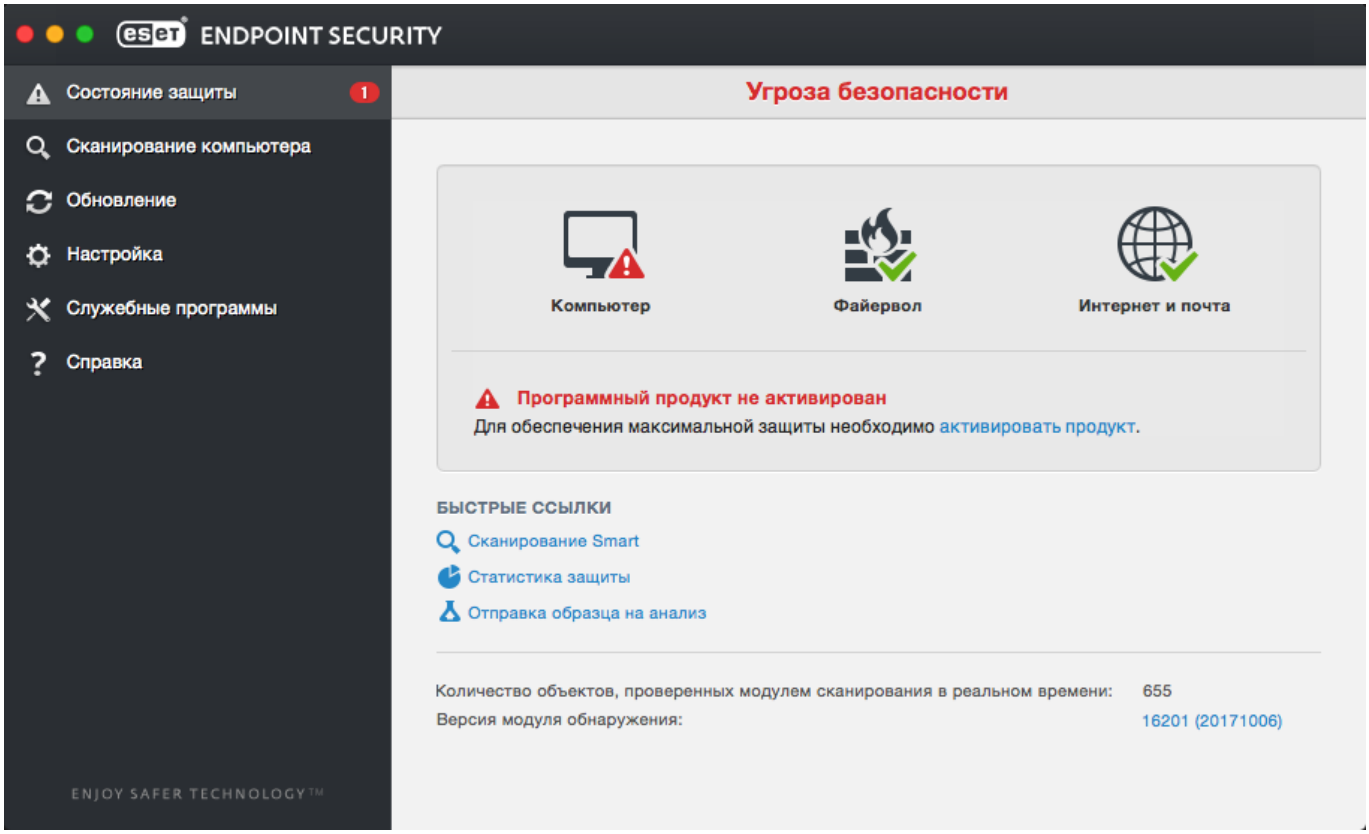
- *cmd+,*: отображает настройки ESET Endpoint Security for macOS.
- *cmd+O* — восстановление размера по умолчанию главного окна программы ESET Endpoint Security for macOS и его перемещение в центр экрана.
- *cmd+Q*: позволяет скрыть главное окно графического интерфейса программы ESET Endpoint Security for macOS. Его можно открыть, щелкнув значок программы ESET Endpoint Security for macOS в строке меню macOS (вверху экрана).
- *cmd+W* — закрытие главного окна программы ESET Endpoint Security for macOS.

Нижеперечисленные сочетания клавиш работают, только если включен параметр **Использовать обычное меню** в меню **Настройка** > **Задать настройки приложения...** > **Интерфейс**:

- *cmd+alt+L*: открывается раздел **Файлы журнала**.
- *cmd+alt+S*: открывается раздел **Планировщик**.
- *cmd+alt+Q*: открывается раздел **Карантин**.

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 for macOS.



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 for macOS.

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**.

Защита от вирусов и шпионских программ

Эта система обеспечивает защиту от вредоносных атак, изменяя файлы, потенциально представляющие угрозу. При обнаружении вредоносного кода модуль защиты от вирусов обезвреживает его, блокируя его выполнение, а затем очищая, удаляя или помещая на

карантин.

Общие

В разделе **Общие** (**Настройка** > **Настроить параметры приложения...** > **Общие**) можно включить обнаружение приложений следующих типов.

- **Потенциально нежелательные приложения**: такие приложения не обязательно являются вредоносными, но могут тем или иным образом снижать производительность системы. Такие приложения обычно запрашивают при установке 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, нажмите кнопку **Настройка**.

Исключения

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

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 *** и *?*) либо выберите папку или файл в структуре дерева.

-  : удаление выбранных записей.
- **По умолчанию**: откат исключений к последнему сохраненному состоянию.

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

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 или после успешного обновления модулей. 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.

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) 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 **открытии**, **создании** и **выполнении**. Рекомендуется не изменять эти настройки по умолчанию, поскольку они обеспечивают максимальную защиту компьютера в режиме реального времени. Защита 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 for macOS, расположенный в строке меню (в верхней части экрана) и выбрав вариант **Отключить защиту файловой системы в реальном времени**. Кроме того, функцию защиты файловой системы в режиме реального времени 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.

- **локальные диски** — системные жесткие диски;
- **съемные носители** — компакт- и DVD-диски, USB-устройства, Bluetooth-устройства и т. д.;
- **сетевые носители** — все подключенные диски.

Рекомендуется использовать параметры по умолчанию и изменять исключения из сканирования только в особых случаях, например, когда сканирование определенных носителей значительно замедляет передачу данных.

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

Расширенные параметры

В этом окне можно определить, какие типы объектов сканируются модулем ThreatSense. Чтобы узнать подробнее о **самораспаковывающихся архивах**, **программах сжатия исполняемых файлов** и **расширенной эвристике**, см. раздел Настройка параметров модуля ThreatSense.

Изменять что-либо в разделе **Параметры сканирования архивов по умолчанию** не рекомендуется. Исключениями могут быть те 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 LiveGrid® 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.

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 for macOS 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**).

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 Security Management Center, 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 for macOS;
- дата и версия модуля обнаружения;
- путь к серверу обновлений.

> **Использование терминала**
> Использование терминала рекомендуется только для опытных пользователей.

Действия, которые следует выполнить, если модуль защиты в режиме реального времени не работает

В этом разделе описаны проблемные ситуации, которые могут возникнуть при использовании функции защиты в режиме реального времени, а также способы их разрешения.

Защита в режиме реального времени отключена

Если защита в режиме реального времени случайно отключена пользователем, ее нужно включить. Чтобы выполнить повторную активацию защиты в режиме реального времени, выберите **Настройка** > **Компьютер** и установите для параметра **Защита файловой системы в режиме реального времени** значение **ВКЛЮЧЕНО**. Кроме того, защиту файловой системы в режиме реального времени 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 очищает заражения

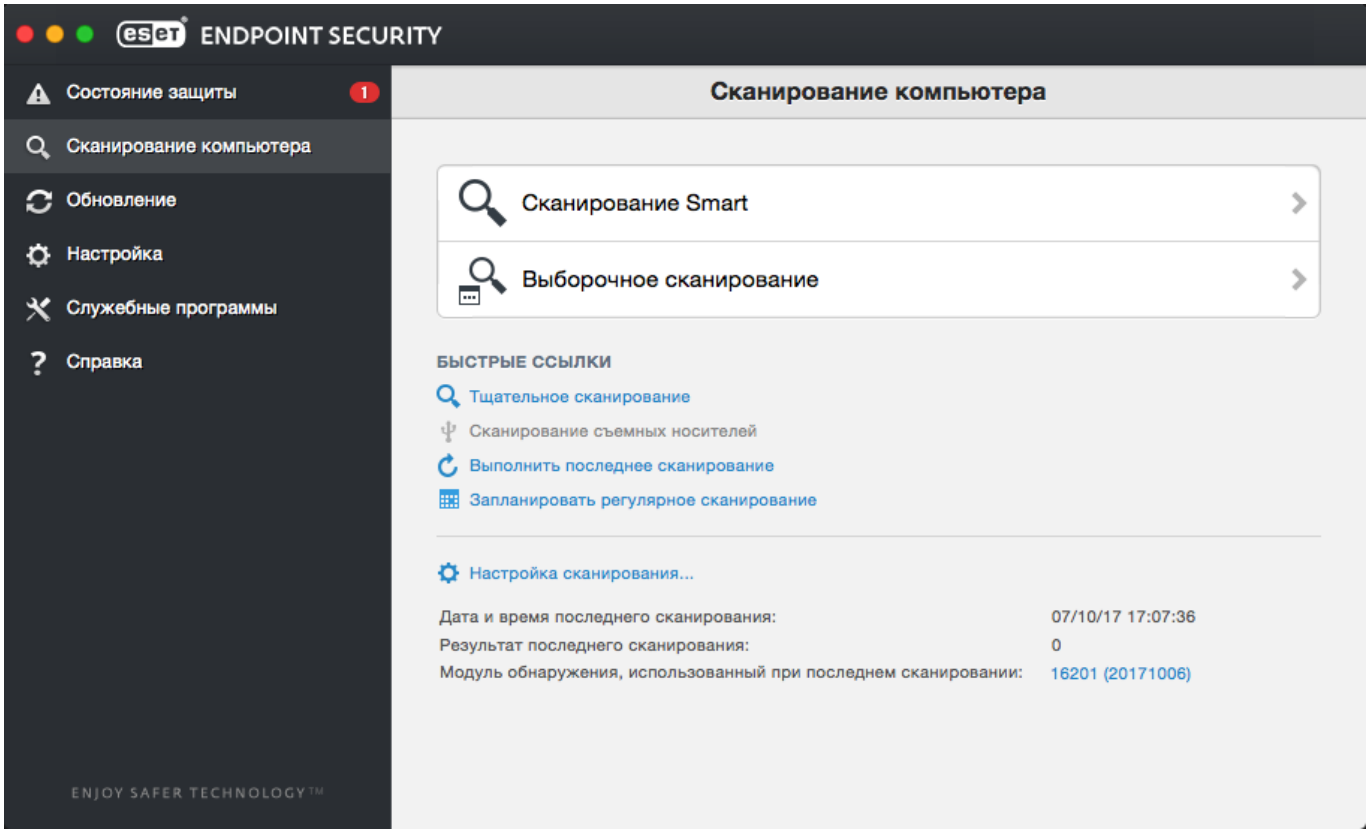
Убедитесь, что на компьютере не установлены другие программы защиты от вирусов. При одновременной работе двух систем защиты в режиме реального времени могут возникать конфликты. Рекомендуется удалить все другие программы защиты от вирусов.

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.

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 во время заражения или если используются устаревшие модули.



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 for macOS, значок Dock, значок в строке меню (в верхней части экрана) или значок приложения (в папке */Applications*).

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.

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.

Выборочное сканирование

Выборочное сканирование позволяет указать параметры сканирования, в частности объекты и методы сканирования. Преимуществом этого типа сканирования является возможность детальной настройки параметров. Различные конфигурации можно сохранить в виде пользовательских профилей сканирования, что может быть полезно 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 только просканировать систему без дополнительных действий по очистке, выберите параметр **Сканировать без очистки**. Кроме того, можно выбрать один из трех уровней очистки, последовательно щелкнув элементы **Настройка** > **Очистка**.

> **Выборочное сканирование**
> Пользователям, не имеющим достаточного опыта работы с антивирусными программами, не рекомендуется выполнять выборочное сканирование.

Объекты сканирования

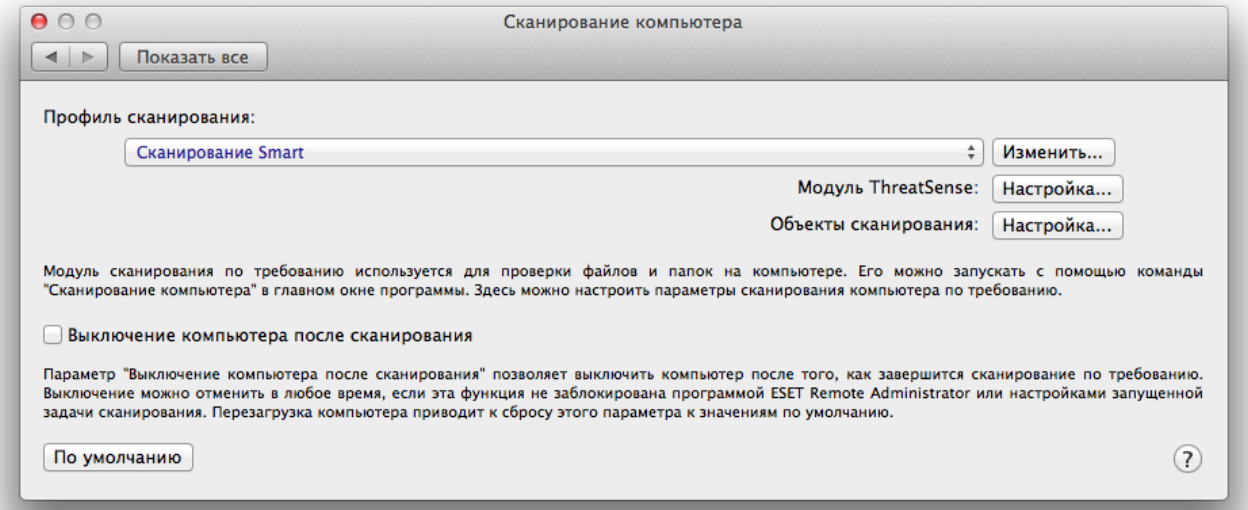
Дерево объектов сканирования позволяет выбирать файлы и папки, которые нужно проверить на наличие вирусов. Выбор папок может осуществляться также в соответствии с параметрами профиля.

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.

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** > **Настроить параметры приложения...** (или нажмите *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, 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 — **OK**. 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**.

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 и пр.), 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 различных методов обнаружения;
- 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 файловой системы 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.

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 этой 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).

- **Программы сжатия исполняемых файлов**: 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).

Параметры

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

- **Эвристический анализ**: эвристические алгоритмы анализируют активность программ на предмет вредоносных действий. Основным преимуществом эвристического анализа является возможность обнаруживать новое вредоносное программное обеспечение, о котором нет никаких сведений.

- **Расширенный эвристический анализ**: 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.

Очистка

Параметры очистки определяют способ очистки зараженных файлов модулем сканирования. Предусмотрено три уровня очистки.

- **Без очистки**: зараженные файлы не очищаются автоматически. Программа выводит предупреждение и предлагает выбрать нужное действие.

- **Стандартная очистка**: программа пытается 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. Исключение составляют только системные файлы. Если очистка файла невозможна, пользователь получает соответствующее уведомление и предложение выбрать требуемое действие.

> ⚠ **Режим стандартной очистки с очисткой архивов**
> 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.

Исключения

Расширением называется часть имени файла, отделенная от основной части точкой. Расширение определяет 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.

Иногда может быть необходимо исключить файлы из сканирования, если сканирование определенных типов файлов препятствует нормальной работе программы. Например, иногда целесообразно исключить из сканирования файлы *log*, *cfg* и *tmp*. Правильный формат ввода расширений:

log

cfg

tmp

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, равное 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.

Другие

Включить оптимизацию Smart

При включенном параметре «Оптимизация Smart» используются оптимальные настройки для обеспечения самого эффективного уровня сканирования без замедления его скорости. Разные модули защиты выполняют интеллектуальное сканирование с применением различных методов. Оптимизация Smart не является жестко заданной для программы. Коллектив разработчиков компании ESET постоянно вносит в нее изменения, которые затем добавляются в ESET Endpoint Security for macOS с помощью регулярных обновлений. Если оптимизация Smart отключена, при сканировании используются только пользовательские настройки ядра ThreatSense каждого 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.

Действия при обнаружении заражения

Заражение может произойти 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 **Сканирование компьютера**.

2. Выберите параметр **Сканирование Smart** (дополнительную информацию см. в разделе Сканирование Smart).

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 for macOS 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.

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.**

> **Исключения при сканировании**
> ESET Endpoint Security for macOS не сканирует зашифрованные протоколы HTTPS, POP3S и IMAPS.

- **Защита доступа в Интернет**: отслеживает обмен данными по протоколу HTTP между веб-браузерами и удаленными серверами.
- **Защита почтового клиента**: позволяет контролировать обмен сообщениями электронной почты по протоколам POP3 и IMAP.
- **Защита от фишинга**: блокирует потенциальные фишинговые атаки с веб-сайтов или доменов.
- **Контроль доступа в Интернет**: блокирует веб-страницы, которые могут содержать неприемлемые или опасные материалы.

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).

Фильтрацию веб-содержимого можно обеспечить, определив номера портов, которые используются для обмена данными по протоколу HTTP и/или URL-адреса.

Порты

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

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.

Защита электронной почты

Защита электронной почты позволяет контролировать обмен сообщениями через протоколы POP3 и IMAP. При проверке входящих сообщений ESET Endpoint Security for macOS использует современные методы сканирования, которые обеспечивает модуль сканирования ThreatSense. Сканирование обмена сообщениями по протоколам POP3 и IMAP выполняется при использовании любого 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 в него может быть добавлено уведомление, содержащее результаты сканирования. Нельзя полагаться исключительно на эти уведомления, 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**: уведомление о выполненной проверке добавляется только в сообщения, содержащие вредоносные программы.
- **Ко всем сканируемым сообщениям**: ESET Endpoint Security for macOS 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.

- %avstatus%: добавляет данные о состоянии заражения письма (например, чистое, заражено и т. д.)
- %virus%: добавляет название угрозы
- %product%: добавляет название вашего продукта ESET (в данном случае — ESET Endpoint Security for macOS)
- %product_url%: добавляет ссылку на веб-сайт ESET (www.eset.com)

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

- Проверка протокола POP3
- Проверка протокола IMAP

Проверка протокола POP3

Протокол POP3 является самым распространенным протоколом, используемым для получения сообщений в клиентских приложениях для работы с электронной почтой. ESET Endpoint Security for macOS 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.

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 for macOS 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.

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** > **Дополнительные настройки...** > **Защита от фишинга**). Все потенциальные фишинговые атаки с опасных веб-сайтов или доменов блокируются, после чего отображается уведомление об атаке.

Файервол

Файервол контролирует весь входящий и исходящий сетевой трафик компьютера, 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.

> **Исключения при сканировании**
> ESET Endpoint Security for macOS не сканирует зашифрованные протоколы HTTPS, POP3S и IMAPS.

Конфигурацию файервола можно найти, последовательно выбрав элементы **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**, 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.

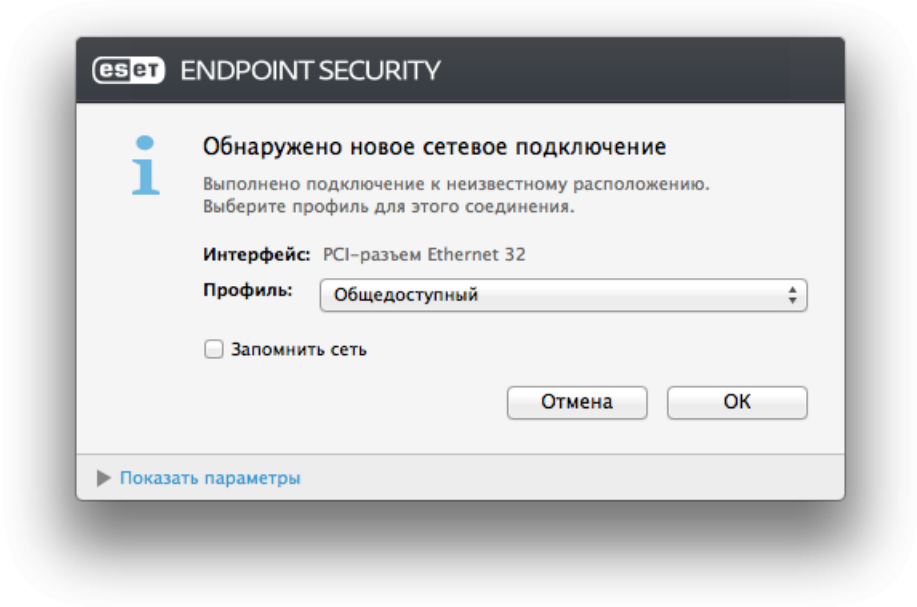
Режимы фильтрации

В файерволе ESET Endpoint Security for macOS 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: все входящие и исходящие соединения будут блокироваться.

Автоматический режим 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 правила, определенные пользователем.

Интерактивный режим: позволяет создать собственную конфигурацию 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 новое правило для файервола. 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**.

Правила файервола

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

Входящее подключение инициируется удаленным компьютером, который пытается установить соединение с локальной системой. При исходящем соединении локальный компьютер пытается подключиться к удаленному.

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. Файервол дает пользователю возможность обнаружить и разорвать такие подключения.

Разрешить программам, подписанным Apple, автоматический доступ к сети: по умолчанию приложения, подписанные Apple, получают доступ к сети автоматически. Чтобы обеспечить возможность взаимодействия приложения со службами Apple или его установки на устройствах, это приложение должно быть подписано с помощью сертификата, выпущенного компанией Apple. Чтобы отключить эту возможность, снимите этот флажок. Чтобы приложения, не подписанные с помощью сертификата Apple, могли получать доступ к сети, будет требоваться действие пользователя или наличие правила.

Когда этот параметр отключен, для обмена данными по сети со службами, подписанными Apple, будет требоваться разрешение пользователя, если оно не будет определено правилом файервола.

Решение ESET Endpoint Security for macOS 6.8 и более ранних версий блокировало входящий обмен данными со службами, которые имели сертификат Apple. Текущая версия решения ESET Endpoint Security for macOS способна определять локального получателя входящего соединения, и если этот параметр включен, входящий обмен данными разрешается.

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 for macOS 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. В завершение необходимо указать параметры **места назначения** (IP-адрес, диапазон, подсеть, сеть Ethernet или Интернет).

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.

Профили файервола

С помощью **профилей** можно контролировать поведение файервола ESET Endpoint Security for macOS. Создавая или изменяя правило для 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 поведение файервола.

Журналы файервола

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

Файлы журнала представляют собой незаменимый инструмент для обнаружения ошибок и выявления вторжений на компьютер. Журналы файервола ESET содержат следующие сведения:

- дата и время события;
- имя события;
- источник;
- сетевой адрес целевого объекта;
- сетевой протокол связи;
- применяемое 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 файервола. Среди этих факторов можно назвать частые подключения с неизвестных компьютеров, множественные попытки установить соединение, сетевая активность неизвестных приложений или использование неизвестных номеров портов.

Контроль устройств

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

> **Контроль устройств в macOS 11 и более поздних версиях**
> Программа ESET Endpoint Security for macOS, установленная в macOS 11 и более поздних версиях, сканирует только накопители (например, USB-накопители, компакт-диски, DVD-диски и т. д.).

Поддерживаемые внешние устройства в macOS 10.15 и более поздних версиях:

- 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 for macOS в разделе **Служебные программы** > **Файлы журнала**.

Редактор правил

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

Если щелкнуть параметр **Включить контроль устройств**, в ESET Endpoint Security for macOS будет активирована функция контроля устройств. Как только контроль устройств будет включен, вы сможете управлять ролями контроля устройств и изменять их. Чтобы включить или 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 ближе к началу списка. Чтобы изменить порядок, достаточно перетащить правило на новое место или щелкнуть  и выбрать нужный параметр.

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

Некоторые устройства можно разрешить или заблокировать на основании сведений об их пользователе, группе пользователя 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 в раскрывающемся меню тип внешнего устройства. Сведения о типе устройства поступают из операционной системы. К накопителям относятся внешние диски и традиционные устройства чтения карт памяти, подключенные по протоколу USB или FireWire. Примерами устройств для обработки изображений служат сканеры и камеры. Так как 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. Напротив, правила для устройств хранения данных позволяют выбрать одно из указанных ниже прав.

Чтение и запись — будет предоставлен 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. Имя 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.

> **Параметры не заданы**
> 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**
> Чтобы просмотреть сведения об устройстве, создайте правило для соответствующего типа устройства и подключите устройство к компьютеру. После подключения устройства сведения о нем отобразятся в журнале контроля устройств.

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.

Нет. 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, правила будут работать для всех пользователей.

> **Ограничения пользовательских правил**
> Не все устройства можно фильтровать по пользовательским правилам (например, устройства для обработки изображений предоставляют информацию только о действиях, но не о пользователях).

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.

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 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.

Служебные программы

Меню **Служебные программы** включает в себя модули, которые облегчают администрирование программы и предлагают дополнительные параметры для опытных пользователей.

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 for macOS.

Получить доступ к файлам журналов можно из главного окна ESET Endpoint Security for macOS (**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 for macOS.

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 файервола отображаются все попытки удаленных атак, которые обнаружил 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 распределении по категориям.

7. **Отфильтрованные веб-сайты**: этот список используется для просмотра списка веб-сайтов, заблокированных функцией защиты доступа в Интернет. иликонтроля доступа в Интернет. 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 нужный файл правой кнопкой мыши и выберите пункт **Копировать**.

Обслуживание журналов

Попасть в раздел настроек ведения журналов ESET Endpoint Security for macOS можно из главного окна приложения. Последовательно выберите элементы **Настройка** > **Дополнительные настройки** > **Служебные программы** > **Файлы журналов**. Для файлов журналов можно настроить несколько параметров.

- **Автоматически удалять устаревшие записи журнала**: записи в журнале старше указанного времени (в днях) автоматически удаляются.

- **Автоматически оптимизировать файлы журналов**: 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, выбранных в разделе **Текстовые журналы**: **изменить**, можно сохранять журналы с записью следующих данных.

- Такие события, как Неверное имя пользователя и пароль, Не удается обновить модули и т. д., записываются в файл *eventslog.txt*.

- Угрозы, обнаруженные с помощью модулей 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.

Фильтрация журнала

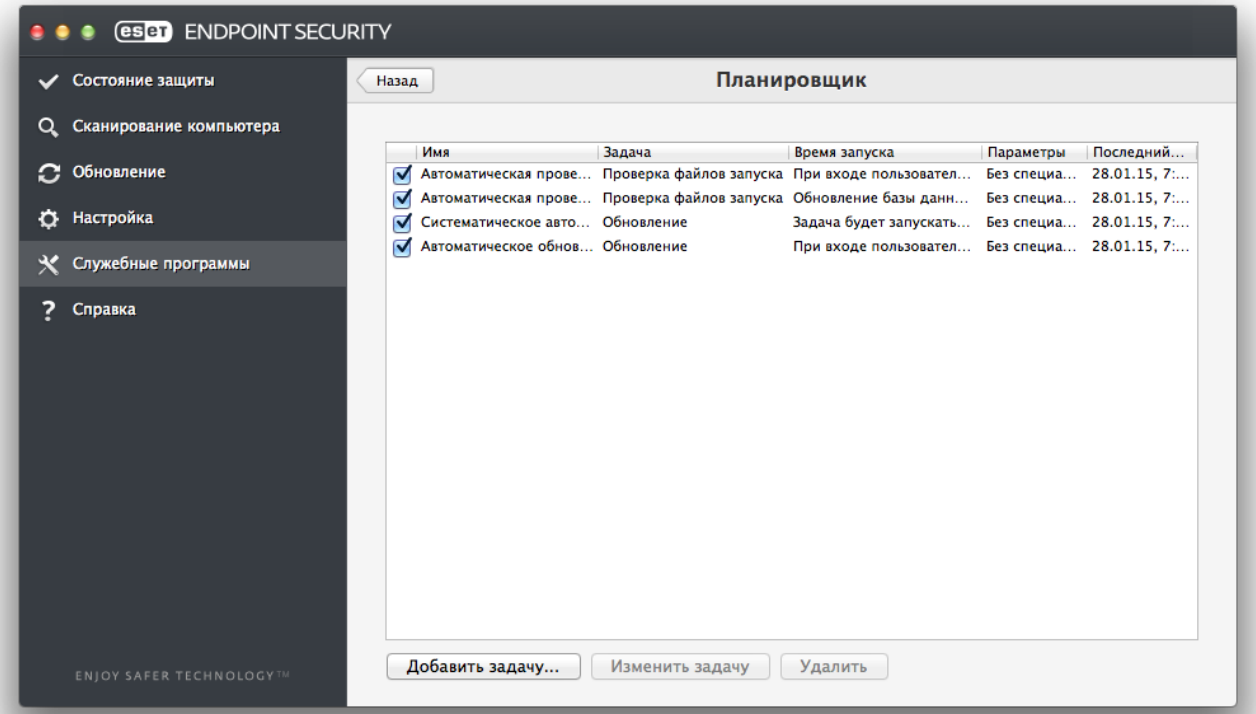
В журналах хранится информация о важных системных событиях. Функция фильтрации журнала позволяет отобразить записи только об определенных событиях.

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 типа «Не удалось загрузить файл» 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.

Планировщик

Планировщик можно найти в главном меню ESET Endpoint Security for macOS 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 при запуске системы после обновления модулей обнаружения
- 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 задачу, удерживая нажатой клавишу CTRL, и выберите команду **Изменить** или выберите задачу и щелкните **Изменить задачу**.

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**. Для планирования доступно четыре типа задач:

- **запуск приложения;**
- **обновление;**
- **сканирование компьютера по требованию;**
- **проверка файлов при загрузке системы.**

Пользовательские задачи

По умолчанию приложения запускаются от имени специально созданного пользователя ESET, который обладает ограниченными правами. Чтобы вместо пользователя по умолчанию указать другого пользователя, введите его имя, добавьте двоеточие (:) и введите команду. В этом случае также можно указать пользователя **root**.

Пример запуска приложения от имени определенного пользователя

В этом примере мы запланируем запуск приложения «Калькулятор» в определенное время от имени пользователя **UserOne**.

1. В окне **Планировщик** щелкните **Добавить задачу**.
2. Введите имя задачи. В списке **Запланированная задача** выберите **Запуск задачи**. В окне **Запуск задачи** щелкните **Раз**, чтобы запустить эту задачу один раз. Нажмите кнопку **Далее**.
3. Щелкните «Обзор» и выберите приложение «Калькулятор».
4. Введите **UserOne:** перед путем к приложению (UserOne:'/Applications/Calculator.app/Contents/MacOs/Calculator') и нажмите кнопку **Далее**.
5. Выберите время запуска задачи и нажмите кнопку **Далее**.
6. Выберите альтернативный вариант на случай, если задача не сможет запуститься, и нажмите кнопку **Далее**.
7. Нажмите кнопку **Готово**.
8. Планировщик ESET запустит приложение «Калькулятор» в указанное время.

Ограничения для имен пользователей

Перед именем пользователя нельзя ставить пробелы. Пробелы также нельзя использовать в именах пользователей. В пустом месте необходимо использовать символ пробела.

Сканирование от имени владельца каталога

Каталоги можно сканировать от имени владельца каталога:
root:for VOLUME in /Volumes/*; do sudo -u \#`stat -f %u "$VOLUME"` '/Applications/ESET Endpoint Security.app/Contents/MacOS/esets_scan' -f /tmp/scan_log "$VOLUME"; done

Кроме того, папку /tmp можно сканировать от имени вошедшего в систему пользователя:
root:sudo -u \#`stat -f %u /dev/console` '/Applications/ESET Endpoint Security.app/Contents/MacOS/esets_scan' /tmp

Пример задачи обновления

В этом примере мы создадим задачу обновления, которая запустится в определенное время.

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 будет предложено выбрать 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).
4. Затем укажите, какое действие следует предпринять, если задача не может быть выполнена в запланированное время.
5. Нажмите кнопку **Готово**. Новая задача появится в списке запланированных.

В программе ESET Endpoint Security for macOS предусмотрены уже готовые запланированные задачи, которые призваны обеспечивать правильную работу приложения. Изменять эти задачи нельзя, и по умолчанию они скрыты. Чтобы просмотреть эти задачи, в главном меню последовательно щелкните элементы **Настройка** > **Дополнительные настройки** > **Планировщик** и установите флажок **Показывать системные задачи**.

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)

Пример.

```
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.

Названия дней ((Monday-Sunday)) и месяцев ((January-December)) не поддерживаются.

Пользовательские задачи

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

LiveGrid®

Система своевременного обнаружения LiveGrid® позволяет компании ESET постоянно и без промедления получать информацию о новых заражениях. Двунаправленная система своевременного обнаружения LiveGrid® 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 модулей обнаружения. В настройках LiveGrid® пользователи могут выбрать один их двух вариантов действий.

1. Систему своевременного обнаружения LiveGrid® можно не включать. Функциональность программного обеспечения при этом не ограничивается, но в некоторых случаях ESET Endpoint Security for macOS может быстрее реагировать на новые угрозы, чем обновление модулей обнаружения.

2. Систему своевременного обнаружения LiveGrid® 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 LiveGrid® будет собирать информацию о компьютере, которая имеет отношение к новым обнаруженным угрозам. Это может быть образец или копия файла, в котором возникла угроза, путь к такому файлу, его имя, дата и время, имя процесса, в рамках которого угроза появилась на компьютере, и сведения об операционной системе.

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

Подозрительные файлы

По умолчанию программа ESET Endpoint Security for macOS 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** > **Дополнительные настройки** > **LiveGrid®** > **Настройка**).

При обнаружении подозрительного файла его можно отправить в нашу лабораторию на анализ. Для этого в главном окне программы выберите **Сервис** > **Отправить файл на анализ**.

Если файл окажется вредоносным приложением, после следующего обновления программа будет его распознавать.

Отправка анонимных статистических данных: система своевременного обнаружения ESET LiveGrid® 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 отправленных статистических данных

```
# 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 исключений: этот параметр позволяет не отправлять файлы определенного типа. 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.

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

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 for macOS 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 for macOS. В папке карантина файлы хранятся в безопасном зашифрованном виде. Их можно восстановить после повторной установки приложения ESET Endpoint Security for macOS.

Помещение файлов на карантин

Программа ESET Endpoint Security for macOS 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 for macOS — добавление файлов в карантин».

Восстановление 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**.

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**.

Права

Настройки ESET Endpoint Security for macOS 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**.

> **Пустой список пользователей с правами**
> Если список пользователей с правами пуст, изменять настройки приложения могут все пользователи системы.

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 for macOS станет оранжевым, чтобы тем самым предупредить вас.

Интерактивный режим и режим презентации в файерволе

Если 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 задать правило подключения для каждого приложения, которое может конфликтовать с таким поведением, или использовать другой режим фильтрации в 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.

Запущенные процессы

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

- **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 for macOS и технология ESET LiveGrid® 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 LiveGrid®.

- **Время обнаружения**: время, прошедшее с того момента, когда приложение было обнаружено технологией ESET LiveGrid®.

- **ИД пакета приложения**: имя поставщика или процесса приложения.

Если щелкнуть определенный процесс, в нижней части окна появится следующая информация.

- **Файл**: расположение приложения на компьютере.

- **Размер файла**: физический размер файла на диске.

- **Описание файла**: характеристики файла на основании описания из операционной системы.

- **ИД пакета приложения**: имя поставщика или процесса приложения.

- **Версия файла**: информация от издателя приложения.

- **Имя программы**: название приложения и/или фирменное наименование.

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 for macOS при запуске системы установите флажок **Показывать заставку при запуске**.

- С помощью параметра **Поместить приложение на панель Dock** можно разместить значок

ESET Endpoint Security for macOS  на панели Dock в ОС macOS и переключаться между программой ESET Endpoint Security for macOS и другими запущенными приложениями с помощью сочетания клавиш *cmd+tab*. Изменения вступают в силу после повторного запуска программы ESET Endpoint Security for macOS (обычно после перезагрузки компьютера).

• Параметр **Использовать обычное меню** позволяет использовать определенные сочетания клавиш (см. раздел Сочетания клавиш) 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 for macOS 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 for macOS  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 for macOS (обычно после перезагрузки компьютера).

Предупреждения и уведомления

В разделе **Предупреждения и уведомления** можно настроить то, как программа ESET Endpoint Security for macOS 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.

Флажок **Отображать уведомления на рабочем столе** обеспечит 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 for macOS 6.2, также появилась возможность отключить отображение определенных **состояний защиты** в главном окне программы (окно **Состояние защиты**). Подробные сведения об этом см. в разделе Состояния защиты.

Отображение предупреждений

В ESET Endpoint Security for macOS отображаются диалоговые окна с предупреждениями, которые информируют пользователя о новых версиях программы, обновлениях ОС, отключении определенных компонентов программы, удалении журналов и т. д. Подобные уведомления

можно отключить, установив для каждого из них 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 for macOS. Чтобы включить или отключить определенное уведомление, установите флажок слева от элемента **Имя диалогового окна**. Когда флажок установлен, уведомление будет отображаться всегда, а **условия отображения** применяться не будут. Если вы не желаете получать уведомление об определенном событии в списке, снимите этот флажок. Кроме того, можно задать **условия отображения**, согласно которым будет выполняться определенное действие.

Состояния защиты

Текущее состояние защиты программы ESET Endpoint Security for macOS можно изменить путем активации или деактивации состояний. Для этого нужно выбрать **Настройка** > **Задать настройки приложения...** > **Предупреждения и уведомления** > **Отображать в окне «Состояние защиты»: настройка**. Состояние различных компонентов программы будет отображено или скрыто в главном окне программы ESET Endpoint Security for macOS (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.

Контекстное меню

Чтобы сделать некоторые функции ESET Endpoint Security for macOS 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.

Обновление

Для обеспечения максимального уровня безопасности необходимо регулярно обновлять ESET Endpoint Security for macOS. Модуль обновления поддерживает актуальное состояние программы, загружая последнюю версию модулей обнаружения.

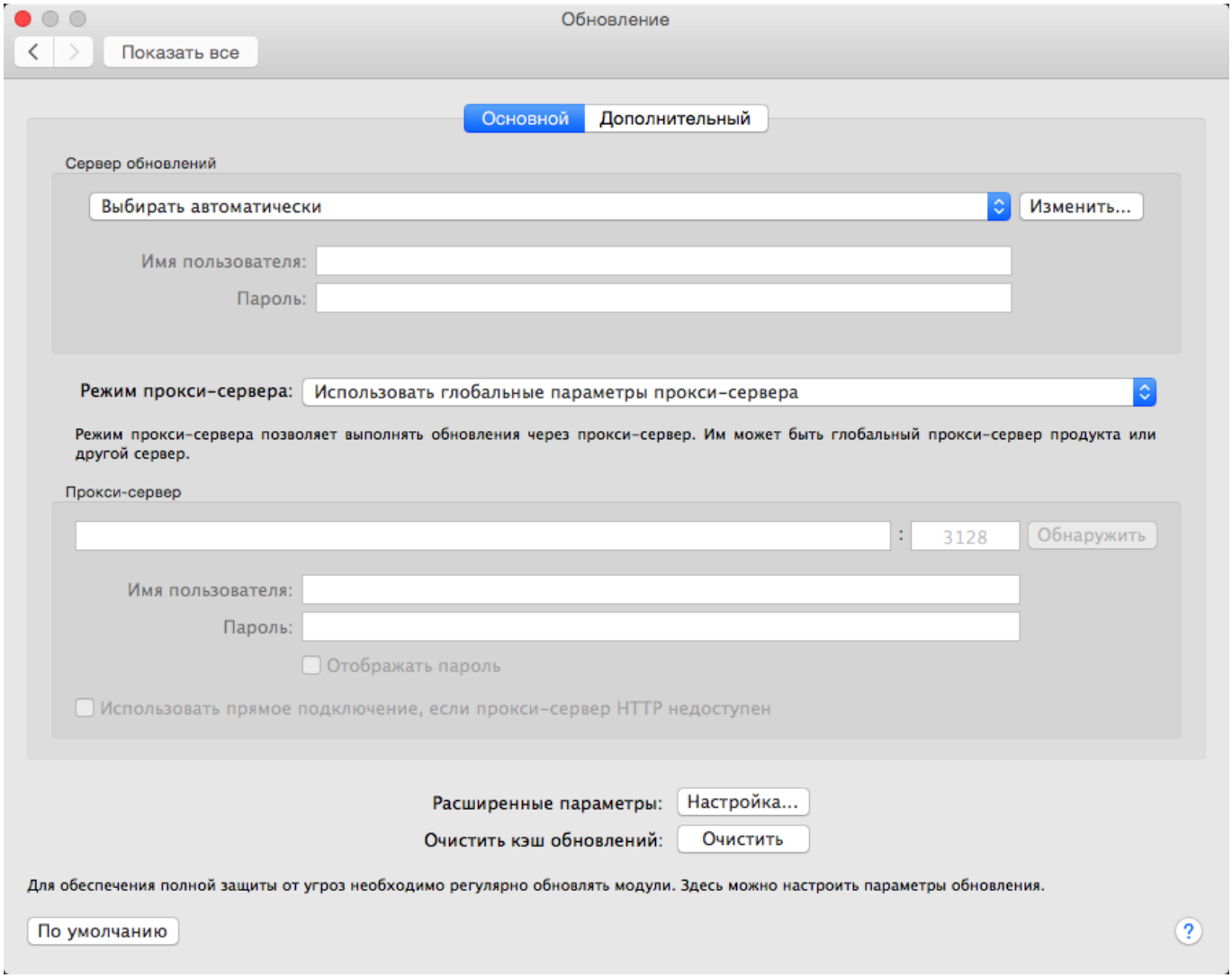
Чтобы просмотреть информацию о текущем состоянии обновления, в том числе дату и время последнего обновления, а также сведения о необходимости обновления, щелкните в главном меню элемент **Обновление**. Чтобы начать процесс обновления вручную, щелкните **Обновление модулей**.

Если у вас установлены последние версии модулей, после корректного завершения загрузки в окне обновления обычно выводится сообщение Обновление не требуется — установлены актуальные версии модулей. Если обновить модули не удается, рекомендуется проверить настройки обновления. Самая распространенная причина такой ошибки — неверно введенные данные лицензии или неправильные параметры подключения.

В окне **Обновление** также указывается версия модуля обнаружения. Этот числовой индикатор представляет собой ссылку на веб-сайт ESET, на котором указаны сведения об обновлении модуля обнаружения.

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 for macOS можно настроить альтернативный (резервный) сервер обновлений. Например, **основным сервером** может быть зеркальный сервер, 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 for macOS будет автоматически выбирать наиболее подходящий сервер обновлений.

Режим прокси-сервера позволяет обновлять модули обнаружения, используя 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 меню Настройка прокси-сервера.

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

1. В раскрывающемся меню выберите **Подключение через прокси-сервер**.

2. Щелкните **Обнаружить**, чтобы программа ESET Endpoint Security for macOS сама ввела IP-адрес и номер порта (порт по умолчанию используется порт **3128**).

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

Программа ESET Endpoint Security for macOS считывает 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 for macOS будет автоматически пытаться подключиться к серверам обновления без использования прокси-сервера. Этот параметр рекомендуется использовать мобильным пользователям, которые используют ноутбуки MacBook.

Если при загрузке обновлений для модулей обнаружения возникли затруднения, щелкните **Очистить кэш обновлений**, чтобы удалить временные файлы обновления.

Расширенные параметры

Чтобы отключить показ оповещений после каждого обновления, установите флажок **Не отображать уведомления о завершении обновления**.

Включите тестовые обновления, что позволит вам 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 их выпуска. Это позволяет убедиться в отсутствии каких-либо ошибок до того, как ваши клиенты получат обновления.

Программа ESET Endpoint Security for macOS создает снимки модуля обнаружения и других программных модулей. Эти снимки используются функцией **отката обновления**. Установленный флажок **Создавать снимки файлов обновлений** позволит программе ESET Endpoint Security for macOS создавать эти снимки автоматически. Если вы подозреваете, что последнее обновление модуля обнаружения и/или программных модулей повреждено или работает нестабильно, вы можете воспользоваться функцией отката обновления до предыдущей версии и отключить обновления на установленный период времени. Или же можно включить ранее отключенные обновления, если они отложены на неопределенный период времени. При использовании функции отката к предыдущему обновлению укажите в раскрывающемся меню «Установить такой период приостановки» время, на которое требуется приостановить загрузку обновлений. Если вы выберете вариант «До отзыва», обычные обновления можно будет возобновить только вручную. Однако следует проявлять осторожность, настраивая период приостановки загрузки обновлений.

Автоматически задавать максимальный возраст модуля обнаружения. С помощью этого параметра можно задать максимальное время (в днях), по истечении которого модули обнаружения будут считаться устаревшими. По умолчанию установлено значение «7 дней».

Создание задач обновления

Последовательно щелкните элементы «Обновление» > **Обновление модулей**, чтобы вручную запустить обновление модулей обнаружения.

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

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 for macOS 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**: отображается оповещение о каждом пропущенном обновлении системы.
- **Показывать только рекомендованные**: отображается оповещение только о рекомендованных обновлениях.

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 for macOS элемент **Установите недостающие обновления**.

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

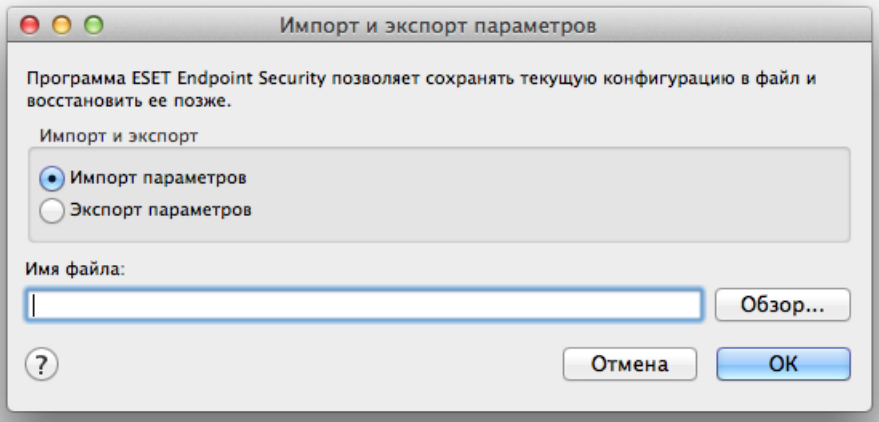
- **[рекомендуется]**: производитель операционной системы рекомендует установить данное обновление, чтобы повысить уровень безопасности и стабильности системы;
- **[перезагрузка]**: после установки обновления необходимо перезагрузить компьютер;
- **[завершение работы]**: после установки обновления требуется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

В окне оповещений отображаются обновления, полученные с помощью инструмента командной строки softwareupdate. Полученные таким образом обновления могут отличаться от обновлений, отображаемых в приложении «Обновления для программного обеспечения». Для того чтобы установить все доступные обновления, отображаемые в окне «Пропущенные обновления системы», а также тех обновления, которые не отображены в приложении «Обновления для программного обеспечения», используйте инструмент командной строки softwareupdate. Чтобы получить дополнительные сведения об инструменте softwareupdate, введите в окне «**Терминал**» команду `man softwareupdate`. Рекомендовано только для опытных пользователей.

Импорт и экспорт параметров

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

Импорт и экспорт удобно использовать, когда нужно создать резервную копию текущей конфигурации ESET Endpoint Security for macOS для дальнейшего использования. Экспорт параметров также можно использовать для переноса желаемой конфигурации ESET Endpoint Security for macOS 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.

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 for macOS. Они используются всеми модулями, которым требуется подключение к Интернету. Программа ESET Endpoint Security for macOS 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**.

Общий локальный кэш

Чтобы активировать использование общего локального кэша, последовательно щелкните «Настройка» > «Дополнительные настройки» > «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. Благодаря этому каждый файл сканируется только один раз, а затем сохраняется в общем кэше. Когда функция активирована, сведения о сканировании файлов и папок в сети сохраняются в локальный кэш. При следующем сканировании продукт ESET Endpoint Security for macOS будет искать сканируемые файлы в кэше. Если файлы совпадают, они будут исключены из сканирования.

Доступны следующие настройки общего локального кэша:

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

> **Подробные инструкции**
> 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.)

Лицензионное соглашение с конечным пользователем

ВАЖНО! Внимательно прочитайте изложенные далее условия использования программного продукта, прежде чем загружать, устанавливать, копировать или использовать его. **ЗАГРУЖАЯ, УСТАНАВЛИВАЯ, КОПИРУЯ ИЛИ ИСПОЛЬЗУЯ ЭТО ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ, ВЫ ВЫРАЖАЕТЕ СВОЕ СОГЛАСИЕ С ИЗЛОЖЕННЫМИ УСЛОВИЯМИ И С ПОЛИТИКА КОНФИДЕНЦИАЛЬНОСТИ.**

Лицезионное соглашение с конечным пользователем

Согласно условиям данного Лицензионного соглашения с конечным пользователем (далее — «Соглашение»), заключенного компанией ESET, spol. s r. o., зарегистрированной по адресу Einsteinova 24, 85101 Bratislava, Slovak Republic, внесенной в коммерческий регистр окружного суда Bratislava I, раздел Sro, запись № 3586/B, BIN 31333532 (далее — «ESET» или «Поставщик»), и вами, физическим или юридическим лицом (далее — «Вы» или «Конечный пользователь»), вы получаете право использовать Программное обеспечение, указанное в статье 1 настоящего Соглашения. Программное обеспечение, указанное в статье 1 настоящего Соглашения, может храниться на носителях данных, отправляться по электронной почте, загружаться через Интернет, загружаться с серверов Поставщика или получаться из других источников, которые удовлетворяют перечисленным ниже условиям.

ЭТО СОГЛАШЕНИЕ КАСАЕТСЯ ПРАВ КОНЕЧНОГО ПОЛЬЗОВАТЕЛЯ И НЕ ЯВЛЯЕТСЯ ДОГОВОРОМ ПРОДАЖИ. Поставщик остается владельцем экземпляра Программного обеспечения и материального носителя, на котором Программное обеспечение было поставлено в торговой упаковке, а также всех копий Программного обеспечения, на которые Конечный пользователь имеет право в соответствии с настоящим Соглашением.

Выбор варианта «Принимаю» в процессе установки, загрузки, копирования или использования этого Программного обеспечения выражает Ваше согласие с условиями настоящего Соглашения. Если Вы не согласны с каким-либо из условий этого Соглашения, немедленно выберите вариант «Не принимаю», отмените установку или загрузку, уничтожьте или верните Программное обеспечение, установочные носители, сопроводительную документацию, а также квитанцию об оплате в компанию ESET или в организацию, в которой было приобретено Программное обеспечение.

ИСПОЛЬЗОВАНИЕ ВАМИ ЭТОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ОЗНАЧАЕТ, ЧТО ВЫ ПРОЧЛИ ДАННОЕ СОГЛАШЕНИЕ, ПОНЯЛИ ЕГО ПОЛОЖЕНИЯ И СОГЛАСНЫ СЧИТАТЬ ИХ ОБЯЗЫВАЮЩИМИ.

1. **Программное обеспечение.** Термин "Программное обеспечение" в настоящем Соглашении означает: (i) компьютерную программу, которая сопровождается настоящим Соглашением, и все ее компоненты; (ii) все содержимое на дисках, компакт-дисках, DVD-дисках, в электронных сообщениях и каких-либо вложениях или на других носителях, которые были поставлены вместе с настоящим Соглашением, в том числе форму объектного кода Программного обеспечения, поставляемую на носителе данных, по электронной почте или загружаемую через Интернет; (iii) любые пояснительные материалы или любую другую возможную документацию, связанную с Программным обеспечением, главным образом какое-либо описание Программного обеспечения, его спецификации, какое-либо описание свойств или работы Программного обеспечения, какое-либо описание рабочей среды, в которой используется Программное обеспечение, инструкции по использованию или установке

Программного обеспечения или какое-либо описание использования Программного обеспечения (далее — Документация); (iv) копии Программного обеспечения, пакеты исправления возможных ошибок Программного обеспечения, дополнения к Программному обеспечению, расширения Программного обеспечения, измененные версии Программного обеспечения и обновления компонентов Программного обеспечения (при наличии), на которые Поставщик предоставил Вам лицензию в соответствии со статьей 3 настоящего Соглашения. Программное обеспечение предоставляется исключительно в форме исполняемого объектного кода.

2. **Установка, компьютер и лицензионный ключ**. Программное обеспечение, поставляемое на носителе данных, по электронной почте, загруженное через Интернет или с серверов Поставщика или полученное из других источников, подлежит установке. Установка Программного обеспечения должна происходить на должным образом настроенном компьютере, который отвечает минимальным требованиям, изложенным в Документации. Способ установки описан в Документации. Компьютер, на котором выполняется установка, не должен содержать программное или аппаратное обеспечение, которое может негативно повлиять на работу Программного обеспечения. Компьютер означает оборудование, в том числе, среди прочего, персональные компьютеры, ноутбуки, рабочие станции, карманные компьютеры, смартфоны, карманные или другие электронные устройства, для которых разрабатывается Программное обеспечение, на котором его будут устанавливать и/или использовать. Лицензионный ключ означает уникальную последовательность символов, букв, цифр или специальных знаков, предоставляемых конечному пользователю, чтобы разрешить законно использовать Программное обеспечение или его определенную версию либо продлить срок действия Лицензии в соответствии с настоящим Соглашением.

3. **Лицензия**. Если Вы приняли все условия, предусмотренные в настоящем Соглашении, и соблюдаете их, Поставщик предоставляет Вам следующие права (далее — «Лицензия»).

a) **Установка и использование.** Вы получаете неисключительное не подлежащее передаче право установить Программное обеспечение на жесткий диск компьютера или иной носитель для хранения данных, установки и хранения Программного обеспечения в памяти компьютера, а также внедрить, хранить и отображать Программное обеспечение.

b) **Оговорка по количеству лицензий.** Право на использование Программного обеспечения ограничено определенным количеством Конечных пользователей. Под одним Конечным пользователем подразумевается (i) установка Программного обеспечения на один компьютер или (ii) в случае ограничения лицензии количеством почтовых ящиков пользователь компьютера, который принимает электронную почту через пользовательский почтовый агент (далее — «Пользовательский почтовый агент»). Если Пользовательский почтовый агент принимает электронную почту, а затем автоматически распределяет ее среди нескольких пользователей, количество Конечных пользователей должно определяться в соответствии с фактическим количеством пользователей, получающих электронную почту. Если почтовый сервер выполняет функции почтового шлюза, количество Конечных пользователей будет равняться количеству пользователей почтового сервера, которых обслуживает этот шлюз. Если один пользователь владеет несколькими адресами электронной почты (например, при использовании псевдонимов) и принимает почту по ним, а почта не распределяется автоматически клиентом другим пользователям, необходима Лицензия только для одного компьютера. Одну Лицензию нельзя использовать одновременно на нескольких компьютерах. Конечный пользователь имеет право вводить Лицензионный ключ в Программное обеспечение только в той степени, в которой он имеет право использовать Программное обеспечение в соответствии с ограничением по количеству Лицензий, выданных Поставщиком. Лицензионный

ключ считается конфиденциальной информацией. Вы не должны передавать Лицензию третьим сторонам или разрешать третьим сторонам использовать Лицензионный ключ, если это не разрешено настоящим Соглашением или Поставщиком. Если Ваш Лицензионный ключ взломан, немедленно сообщите об этом Поставщику.

c) **Выпуск для бизнеса.** Для использования Программного обеспечения на почтовых серверах, серверах ретрансляции электронной почты, почтовых шлюзах и шлюзах Интернета необходима версия Программного обеспечения для бизнеса.

d) **Срок Лицензии.** Ваше право на использование Программного обеспечения ограничено определенным сроком.

e) **Программное обеспечение, получаемое через изготовителей комплектного оборудования.** Программное обеспечение, получаемое через изготовителей комплектного оборудования, можно использовать только на том компьютере, на котором оно было получено. Такое программное обеспечение нельзя перенести на другой компьютер.

f) **Не предназначенные для продажи и пробные версии Программного обеспечения.** Программное обеспечение, классифицированное как не предназначенная для продажи или пробная версия, не может быть связано с каким-либо платежом и должно использоваться исключительно для демонстрации или тестирования функций Программного обеспечения.

g) **Прекращение действия Лицензии.** Действие Лицензии прекращается автоматически по окончании периода, на который она была выдана. Если Вы нарушаете любое положение настоящего Соглашения, Поставщик получает право выйти из него, что никак не повлияет на его возможности воспользоваться любыми правами и средствами судебной защиты, доступными ему в таких обстоятельствах. В случае отмены Лицензии Вы обязаны немедленно за собственный счет удалить, разрушить или вернуть Программное обеспечение и все его резервные копии в компанию ESET или в организацию, в которой оно было приобретено. В случае прекращения действия Лицензии Поставщик также имеет право запретить Конечному пользователю использовать функции Программного обеспечения, которые требуют подключения к серверам Поставщика или серверам третьих лиц.

4. **Функции, для которых необходим сбор данных и подключение к Интернету.** Для корректной работы Программного обеспечения необходимо подключение к Интернету, поскольку Программное обеспечение должно регулярно подключаться к серверам Поставщика или третьих лиц, а также собирать соответствующие данные в соответствии с документом Политика конфиденциальности. Подключение к Интернету необходимо для использования перечисленных далее функций Программного обеспечения.

a) **Обновление Программного обеспечения.** Поставщик имеет право время от времени выпускать обновления Программного обеспечения («Обновления»), но не обязан их предоставлять. Эта функция включена при использовании стандартных параметров Программного обеспечения. Это значит, что Обновления устанавливаются автоматически, если Конечный пользователь не отключит их автоматическую установку. Для предоставления обновлений необходима проверка подлинности лицензии, включая информацию о компьютере и/или платформе, на которой установлено Программное обеспечение, в соответствии с документом Политика конфиденциальности.

b) **Отправка зараженных файлов и информации Поставщику.** Программное обеспечение оснащено функциями, которые собирают образцы компьютерных вирусов и других вредоносных программ, а также подозрительные, проблемные, потенциально нежелательные

или потенциально опасные объекты, такие как файлы, URL-адреса, IP-пакеты и кадры Ethernet (именуемые в дальнейшем «Заражения»), и отправляют их Поставщику, в том числе, среди прочего, информацию о процессе установки, о компьютере и/или платформе, на которых установлено Программное обеспечение, и/или информацию об операциях и функциональности программного обеспечения, и/или информацию об устройствах локальной сети, например сведения о типе, поставщике, модели и/или названии устройства (далее — «Информация»). Информация и Заражения могут содержать данные (в том числе случайно или непредумышленно полученные персональные данные) о Конечном пользователе или других пользователях компьютера, на котором установлено Программное обеспечение, и о файлах, пораженных Заражениями с соответствующими метаданными.

Информацию и Заражения могут собирать следующие функции Программного обеспечения:

i. Функция LiveGrid Reputation System отвечает за сбор и отправку Поставщику в одном направлении хэшей, связанных с Заражениями. Эта функция включена при использовании стандартных параметров Программного обеспечения.

ii. Система обратной связи LiveGrid отвечает за сбор и отправку Поставщику Заражений со связанными метаданными и Информации. Конечный пользователь может активировать эту функцию в процессе установки Программного обеспечения.

Поставщик обязуется использовать полученные Заражения и Информацию только для анализа и исследования Заражений, улучшения Программного обеспечения и усовершенствования проверки подлинности Лицензии, а также принять необходимые меры предосторожности по сохранению конфиденциальности Информации и Заражений. Активируя эту функцию Программного обеспечения, Вы соглашаетесь на отправку Заражений и Информации Поставщику, а также даете ему необходимое разрешение, регулируемое соответствующими правовыми нормами, на обработку полученной Информации. Данную функцию можно отключить в любой момент.

Для целей настоящего Соглашения необходимо собирать, обрабатывать и хранить данные, позволяющие Поставщику идентифицировать Вас в соответствии с документом Политика конфиденциальности. Настоящим Вы подтверждаете, что Поставщик с помощью своих средств может проверять, используете ли Вы Программное обеспечение в соответствии с положениями настоящего Соглашения. Вы соглашаетесь на передачу информации в процессе обмена данными между Программным обеспечением и компьютерными системами Поставщика или его коммерческих партнеров, входящих в сеть распространения и поддержки Поставщика, с целью обеспечения работы и проверки возможности использования Программного обеспечения и защиты прав Поставщика.

После заключения этого Соглашения Поставщик или любой из его коммерческих партнеров, входящих в сеть распространения и поддержки Поставщика, получат право передавать, обрабатывать и хранить важные данные, позволяющие идентифицировать Вашу личность, в целях оплаты и исполнения настоящего Соглашения, а также для отправки уведомлений на Ваш компьютер. Настоящим Вы соглашаетесь получать уведомления и сообщения в отношении продукта, в том числе информацию рекламного характера.

Сведения о конфиденциальности, защите персональных данных и Ваших правах как субъекта персональных данных приведены в Политике конфиденциальности, которая доступна на веб-сайте Поставщика, а также непосредственно в процессе установки. Вы также можете открыть ее из справки Программного обеспечения.

5. **Использование прав Конечного пользователя**. Права Конечного пользователя необходимо использовать лично, либо их могут использовать Ваши сотрудники. Вы имеете право на использование Программного обеспечения только для защиты своих действий и компьютеров или компьютерных систем, на которые приобретена Лицензия.

6. **Ограничения прав.** Не разрешается копировать, распространять Программное обеспечение, извлекать его компоненты и создавать производные работы на его основе. При использовании Программного обеспечения Вы обязаны соблюдать перечисленные далее ограничения.

a) Вы можете создать одну резервную копию Программного обеспечения на носителе постоянного хранения данных при условии, что эта резервная копия не установлена и не используется ни на каком компьютере. Создание любых иных копий Программного обеспечения является нарушением этого Соглашения.

b) Вы не должны использовать, изменять, переводить или воспроизводить Программное обеспечение и передавать права на использование Программного обеспечения или копии Программного обеспечения любым способом, отличным от описанного в настоящем Соглашении.

c) Вы не должны продавать, передавать на условиях сублицензии, сдавать в аренду или передавать во временное пользование Программное обеспечение, а также использовать Программное обеспечение для предоставления коммерческих услуг.

d) Запрещается вскрывать технологию, декомпилировать или разбирать код Программного обеспечения и иными способами пытаться получить исходный код Программного обеспечения за исключением того, в чем данное ограничение противоречит действующему законодательству.

e) Вы соглашаетесь использовать Программное обеспечение только способом, соответствующим всем действующим законодательным нормам страны, в которой используется Программное обеспечение, в том числе применимым ограничениям относительно авторского права, других прав на интеллектуальную собственность и так далее.

f) Вы соглашаетесь использовать Программное обеспечение и его функции только способом, который не ограничивает возможности доступа к этим услугам других Конечных пользователей. Поставщик оставляет за собой право ограничить объем услуг, предоставляемых отдельным Конечным пользователям, чтобы обеспечить использование услуг максимально возможным числом Конечных пользователей. Ограничение объема услуг должно также означать полное прекращение возможности использовать любую из функций Программного обеспечения, а также удаление Данных и информации на серверах Поставщика или сторонних серверах, относящихся к определенной функции Программного обеспечения.

g) Вы обязуетесь не предпринимать действий, связанных с использованием Лицензионного ключа, которые противоречат условиям настоящего Соглашения или приводят к предоставлению Лицензионного ключа лицу, не имеющему права использовать Программное обеспечение, например передачу использованного или неиспользованного Лицензионного ключа в любой форме, а также несанкционированное воспроизведение или распространение дублированных или сгенерированных лицензионных ключей или использование Программного обеспечения с помощью Лицензионного ключа, полученного не от Поставщика.

7. **Авторское право**. Программное обеспечение и все права на него, в том числе, среди прочего, право собственности и права на объекты интеллектуальной собственности,

принадлежат компании ESET и/или ее лицензиарам. Эти права защищены международными соглашениями и всеми прочими применимыми законодательными нормами страны, в которой используется Программное обеспечение. Внутренняя структура, устройство и код Программного обеспечения являются ценной коммерческой тайной и конфиденциальной информацией, принадлежащими компании ESET и/или ее лицензиарам. Запрещается копировать Программное обеспечение кроме случаев, описанных в статье 6(a). Любые копии, которые разрешено создать в соответствии с Соглашением, должны содержать оригинальные отметки о защите авторских прав и другие уведомления о правах интеллектуальной собственности, которые присутствуют в самом Программном обеспечении. Если Вы вскрываете технологию, декомпилируете, разбираете исходный код Программного обеспечения или иным способом пытаетесь получить исходный код Программного обеспечения в нарушение положений этого Соглашения, любая полученная таким образом информация автоматически и безоговорочно должна считаться подлежащей передаче Поставщику и принадлежащей ему полностью с момента создания вне зависимости от прав Поставщика в отношении нарушения этого Соглашения.

8. **Сохранение прав**. Настоящим Поставщик сохраняет за собой все права на Программное обеспечение, за исключением прав, явно предоставленных Вам как Конечному пользователю Программного обеспечения в соответствии с условиями настоящего Соглашения.

9. **Несколько языковых версий, программное обеспечение на носителях двух типов, несколько копий**. Если Программное обеспечение поддерживает несколько платформ или языков или если Вы получили несколько экземпляров программного обеспечения, разрешается использовать Программное обеспечение только на том количестве компьютеров и в тех версиях, на которые была приобретена Лицензия. Запрещается продавать, передавать на условиях сублицензии, сдавать в аренду, передавать во временное или постоянное пользование версии или копии Программного обеспечения, которые не используются Вами.

10. **Момент вступления в силу и прекращение действия Соглашения**. Настоящее Соглашение вступает в законную силу с дня, когда Вы согласились с его условиями. Завершить действие Соглашения можно в любой момент, необратимо удалив, разрушив или вернув за свой счет Программное обеспечение, все резервные копии и любые относящиеся к нему материалы, предоставленные Поставщиком или одним из его коммерческих партнеров. Независимо от способа прекращения действия этого Соглашения положения статей 7, 8, 11, 13, 19 и 21 остаются действительными без ограничения по времени.

11. **ГАРАНТИИ КОНЕЧНОГО ПОЛЬЗОВАТЕЛЯ**. ВЫСТУПАЯ В КАЧЕСТВЕ КОНЕЧНОГО ПОЛЬЗОВАТЕЛЯ, ВЫ ПОДТВЕРЖДАЕТЕ СВОЮ ОСВЕДОМЛЕННОСТЬ В ТОМ, ЧТО ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ПОСТАВЛЯЕТСЯ НА УСЛОВИЯХ «КАК ЕСТЬ» БЕЗ КАКИХ-ЛИБО ПРЯМЫХ ИЛИ ВМЕНЕННЫХ ГАРАНТИЙ ЛЮБОГО ТИПА, НАСКОЛЬКО ЭТО ПОЗВОЛЯЮТ СООТВЕТСТВУЮЩИЕ ЗАКОНОДАТЕЛЬНЫЕ НОРМЫ. НИ ПОСТАВЩИК, НИ ЕГО ПАРТНЕРЫ, ВЫСТУПАЮЩИЕ В КАЧЕСТВЕ ЛИЦЕНЗИАРОВ ИЛИ АФФИЛИРОВАННЫХ ЛИЦ, НИ ПРАВООБЛАДАТЕЛИ НЕ ДЕЛАЮТ НИКАКИХ ЗАЯВЛЕНИЙ И НЕ ПРЕДОСТАВЛЯЮТ НИКАКИХ ПРЯМЫХ ИЛИ ВМЕНЕННЫХ ОБЯЗАТЕЛЬСТВ ИЛИ ГАРАНТИЙ, В ЧАСТНОСТИ ГАРАНТИЙ ПРОДАЖ ИЛИ ГАРАНТИЙ ПРИГОДНОСТИ ДЛЯ ОПРЕДЕЛЕННОГО ИСПОЛЬЗОВАНИЯ, А ТАКЖЕ ГАРАНТИЙ ТОГО, ЧТО ЭТО ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ НЕ НАРУШАЕТ НИКАКИХ ПАТЕНТОВ, АВТОРСКИХ ПРАВ, ПРАВ НА ТОВАРНЫЕ ЗНАКИ И ДРУГИХ ПРАВ ТРЕТЬИХ ЛИЦ. ПОСТАВЩИК И ЛЮБЫЕ ДРУГИЕ ЛИЦА НЕ ГАРАНТИРУЮТ, ЧТО ФУНКЦИИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ БУДУТ СООТВЕТСТВОВАТЬ ВАШИМ ТРЕБОВАНИЯМ ИЛИ ЧТО ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ БУДЕТ РАБОТАТЬ БЕЗ СБОЕВ И ОШИБОК. РИСК ПРИ ВЫБОРЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ ДОСТИЖЕНИЯ НУЖНЫХ РЕЗУЛЬТАТОВ, А ТАКЖЕ ПРИ УСТАНОВКЕ, ИСПОЛЬЗОВАНИИ И ПОЛУЧЕНИИ РЕЗУЛЬТАТОВ, КОТОРЫХ ВЫ БУДЕТЕ ДОСТИГАТЬ С

ПОМОЩЬЮ ЭТОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, ЛЕЖИТ НА ВАС.

12. **Отказ от других обязательств**. Настоящее Соглашение не предусматривает никаких обязательств для Поставщика и его лицензиаров за исключением тех, которые изложены в настоящем Соглашении.

13. **ОГРАНИЧЕНИЕ ОТВЕТСТВЕННОСТИ**. В ТОЙ СТЕПЕНИ, В КОТОРОЙ ЭТО РАЗРЕШЕНО ПРИМЕНИМЫМ ЗАКОНОДАТЕЛЬСТВОМ, НИ ПРИ КАКИХ ОБСТОЯТЕЛЬСТВАХ ПОСТАВЩИК, ЕГО СОТРУДНИКИ ИЛИ ЛИЦЕНЗИАРЫ НЕ НЕСУТ ОТВЕТСТВЕННОСТИ ЗА КАКУЮ-ЛИБО УПУЩЕННУЮ ПРИБЫЛЬ, ВЫРУЧКУ, ПРОДАЖИ, ДАННЫЕ ИЛИ РАСХОДЫ НА ЗАКУПКУ ВЗАИМОЗАМЕНЯЕМЫХ ТОВАРОВ ИЛИ УСЛУГ, ПОВРЕЖДЕНИЕ ИМУЩЕСТВА, ТЕЛЕСНЫЕ ПОВРЕЖДЕНИЯ, ПРИОСТАНОВКУ РАБОТЫ, ПОТЕРЮ КОММЕРЧЕСКОЙ ИНФОРМАЦИИ ИЛИ ЗА КАКИЕ-ЛИБО ФАКТИЧЕСКИЕ, ПРЯМЫЕ, НЕПРЯМЫЕ, ПОБОЧНЫЕ, ЭКОНОМИЧЕСКИЕ, КОМПЕНСИРУЕМЫЕ, ШТРАФНЫЕ, КОСВЕННЫЕ ИЛИ ПРЕДСКАЗУЕМЫЕ КОСВЕННЫЕ УБЫТКИ, НАНЕСЕННЫЕ В РЕЗУЛЬТАТЕ ВЫПОЛНЕНИЯ СОГЛАШЕНИЯ, ГРАЖДАНСКОГО ПРАВОНАРУШЕНИЯ ИЛИ НЕБРЕЖНОСТИ, НЕЗАВИСИМО ОТ ПРИЧИНЫ И ВИДА ОТВЕТСТВЕННОСТИ, ВОЗНИКАЮЩИЕ В РЕЗУЛЬТАТЕ ИСПОЛЬЗОВАНИЯ ИЛИ ОТСУТСТВИЯ ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, ДАЖЕ ЕСЛИ ПОСТАВЩИК, ЕГО ЛИЦЕНЗИАРЫ ИЛИ АФФИЛИРОВАННЫЕ ЛИЦА ОСВЕДОМЛЕНЫ О ВОЗМОЖНОСТИ ВОЗНИКНОВЕНИЯ ТАКОГО УЩЕРБА. ПОСКОЛЬКУ ЗАКОНОДАТЕЛЬСТВО НЕКОТОРЫХ СТРАН И ОТДЕЛЬНЫЕ ЗАКОНЫ НЕ РАЗРЕШАЮТ ИСКЛЮЧАТЬ ТАКУЮ ОТВЕТСТВЕННОСТЬ, НО ПОЗВОЛЯЮТ ОГРАНИЧИВАТЬ ЕЕ, В ТАКИХ СЛУЧАЯХ ОТВЕТСТВЕННОСТЬ ПОСТАВЩИКА, ЕГО СОТРУДНИКОВ, ЛИЦЕНЗИАРОВ ИЛИ АФФИЛИРОВАННЫХ ЛИЦ ОГРАНИЧИВАЕТСЯ СУММОЙ, ВЫПЛАЧЕННОЙ ВАМИ ЗА ЛИЦЕНЗИЮ.

14. Ни одно из положений настоящего Соглашения не затрагивает законные права любой стороны, выступающей в качестве потребителя, даже если они противоречат таким правам.

15. **Техническая поддержка**. ESET или привлеченные компанией ESET третьи лица предоставляют техническую поддержку по собственному усмотрению без каких-либо гарантий или заявлений. Конечный пользователь обязан создать резервную копию всех существующих данных, программного обеспечения или программных средств, прежде чем обратиться за технической поддержкой. ESET и (или) третьи лица, привлеченные ESET, не могут принять на себя ответственность за повреждение или потерю данных, собственности, программного обеспечения или оборудования, а также за упущенную прибыль, которые связаны с предоставлением технической поддержки. ESET и (или) привлеченные ESET третьи лица оставляют за собой право принять решение о том, что устранить конкретную проблему невозможно в рамках технической поддержки. ESET оставляет за собой право отказать в предоставлении технической поддержки, приостановить или прекратить ее оказание по своему собственному усмотрению. Сведения о лицензии, Информация и другие данные в соответствии с Политикой конфиденциальности могут потребоваться для предоставления технической поддержки.

16. **Передача лицензии**. Программное обеспечение может быть перенесено с одного компьютера на другой, если это не противоречит условиям настоящего Соглашения. Если это не противоречит условиям Соглашения, Конечный пользователь может только перманентно передать Лицензию и все права по настоящему Соглашению другому Конечному пользователю с согласия Поставщика, если соблюдаются следующие условия: (i) у первого Конечного пользователя не остается никаких экземпляров Программного обеспечения; (ii) передача прав должна быть непосредственной, т. е. от исходного Конечного пользователя к новому; (iii) новый Конечный пользователь должен принять все права и обязательства исходного Конечного пользователя по настоящему Соглашению; (iv) исходный Конечный пользователь должен предоставить новому Конечному пользователю документацию, позволяющую проверить

подлинность Программного обеспечения в соответствии со статьей 17.

17. **Проверка подлинности Программного обеспечения**. Конечный пользователь может продемонстрировать наличие у него прав на использование Программного обеспечения одним из следующих способов: (i) с помощью лицензионного сертификата, выданного Поставщиком или третьим лицом, которое назначено Поставщиком; (ii) письменным лицензионным соглашением, если таковое было заключено; (iii) путем предоставления отправленного Поставщиком сообщения электронной почты, в котором содержатся сведения о лицензии (имя пользователя и пароль). Сведения о лицензии и идентификационные данные Конечного пользователя в соответствии с Политикой конфиденциальности могут потребоваться для проверки подлинности программного обеспечения.

18. **Предоставление лицензии органам власти и правительству США**. Программное обеспечение будет предоставлено органам власти, в том числе правительству Соединенных Штатов Америки, в соответствии с правами и ограничениями, описанными в настоящем Соглашении.

19. **Соответствие нормам регулирования внешней торговли**.

a) Вы не будете прямо или косвенно экспортировать, реэкспортировать, передавать или иным образом предоставлять Программное обеспечение кому-либо, а также не будете использовать его каким-либо образом либо иметь отношение к каким-либо действиям, в результате чего компания ESET или ее холдинговые компании, ее филиалы, филиалы ее холдинговых компаний, прочие субъекты, находящиеся под управлением ее холдинговых компаний (далее — «Аффилированные лица»), может стать нарушителем Законодательства по регулированию внешней торговли либо получить негативные последствия в связи с его применением. К законодательству по регулированию внешней торговли относится:

i. Любое законодательство, которое предназначено для регулирования, ограничения или введения лицензионных требований в сфере экспорта, реэкспорта или передачи товаров, программного обеспечения, технологий, услуг и которое принимается любыми правительственными, государственными или регулятивными органами Соединенных Штатов Америки, Сингапура, Великобритании, Европейского Союза или любого входящего в него государства, а также любой страны, в которой должны выполняться обязательства согласно настоящему Соглашению или в которой зарегистрирована либо действует компания ESET или какие-либо ее Аффилированные лица (далее — «Законодательство по регулированию внешней торговли»).

ii. Любые экономические, финансовые, торговые и прочие санкции, ограничения, эмбарго, запреты на импорт или экспорт, запреты на перевод денежных средств или активов либо на предоставление услуг, а также эквивалентные меры, которые вводятся в действие любыми правительственными, государственными или регулятивными органами Соединенных Штатов Америки, Сингапура, Великобритании, Европейского Союза или любого входящего в него государства, а также любой страны, в которой должны выполняться обязательства согласно настоящему Соглашению или в которой зарегистрирована либо действует компания ESET или какие-либо ее Аффилированные лица (далее — «Санкционное законодательство»).

b) Компания ESET имеет право приостановить выполнение своих обязательств согласно настоящим Условиям либо незамедлительно прекратить действие настоящих Условий в следующих случаях:

i. В случае, если компания ESET устанавливает, что по ее обоснованному мнению Пользователь

нарушил или может нарушить положения Статьи 19-а настоящего Соглашения.

ii. В случае, если Конечный пользователь и/или Программное обеспечение попадут под действие Законодательства по регулированию внешней торговли, и, как результат, компания ESET установит, что по ее обоснованному мнению продолжение выполнения своих обязательств согласно настоящему Соглашению может привести к тому, что компания ESET или ее Аффилированные лица может стать нарушителем Законодательства по регулированию внешней торговли либо получить негативные последствия в связи с его применением.

c) Ни одна часть настоящего Соглашения не предназначена, не может интерпретироваться или истолковываться так, чтобы побуждать либо обязывать любую его сторону действовать или воздерживаться от действий (или согласиться действовать или воздерживаться от действий) каким-либо образом, который противоречит любому применимому Законодательству по регулированию внешней торговли, преследуется или запрещается им.

20. **Уведомления**. Все уведомления, возвращаемое Программное обеспечение и документация должны быть доставлены по адресу: ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic.

21. **Применимое законодательство**. Данное Соглашение регулируется и толкуется в соответствии с законодательством Словацкой Республики. Конечный пользователь и Поставщик согласны, что принципы коллизионного права и Конвенция Организации Объединенных Наций о договорах международной купли-продажи товаров не применяются. Вы явным образом соглашаетесь с тем, что эксклюзивная юрисдикция по решению любых споров и вопросов с Поставщиком или относительно способа использования Программного обеспечения принадлежит окружному суду I в Братиславе.

22. **Общие положения**. Если любое положение настоящего Соглашения оказывается недействительным или невыполнимым, это не отражается на действительности остальных положений Соглашения, которые по-прежнему будут действительными и выполнимыми в соответствии с указанными здесь условиями. При наличии расхождений между разными языковыми версиями настоящего Соглашения преимуществом обладает версия на английском языке. Любые поправки к настоящему Соглашению могут иметь место только в письменной форме и должны быть подписаны действующим на основе закона компетентным и уполномоченным представителем Поставщика.

Это полное Соглашение между Поставщиком и Вами относительно использования Программного обеспечения, которое заменяет все предыдущие заверения, обсуждения, гарантии или уведомления или рекламные материалы в отношении Программного обеспечения.

EULA ID: BUS-STANDARD-20-01

Privacy Policy

Компания ESET, spol. s r. o., зарегистрированная по адресу Einsteinova 24, 851 01 Bratislava, Словацкая Республика, внесенная в реестр юридических лиц окружного суда I в Братиславе, раздел Sro, запись № 3586/B, регистрационный номер предприятия 31333532, в качестве оператора данных (далее — «ESET» или «Мы») стремится обеспечить прозрачность своих действий, связанных с обработкой личных данных и обеспечением конфиденциальности клиентов. Поэтому Мы публикуем Политику конфиденциальности, исключительно чтобы уведомить клиента (далее — «Конечный пользователь» или «Вы») о нижеследующем:

- Обработка персональных данных,
- Конфиденциальность данных,
- права субъекта данных.

Обработка персональных данных

Услуги, предоставляемые ESET и реализованные в нашем продукте, предоставляются в соответствии с Лицензионным соглашением с конечным пользователем (далее — «Лицензионное соглашение»), но некоторые из них могут потребовать особого внимания. Мы хотим рассказать Вам подробнее о сборе данных, связанных с предоставлением наших служб. Мы предоставляем различные услуги, описанные в Лицензионном соглашении и документации, например услугу обновления, систему ESET LiveGrid®, защиту от ненадлежащего использования данных, поддержку и т. д. Чтобы все это работало, нам необходимо собирать следующую информацию.

- обновления и другую статистику, содержащую данные о процессе установки и Вашем компьютере, в том числе тип платформы, операции и функции Наших программ, например версию ОС, характеристики оборудования, идентификаторы инсталляций и лицензий, IP- и MAC-адреса, конфигурации программ;
- Однонаправленные хеш-функции, связанные с заражениями и входящие в систему репутации ESET LiveGrid®, которая повышает эффективность решений для защиты от вредоносных программ и благодаря которой сканируемые файлы сопоставляются с элементами белого и черного списков в облаке.
- Подозрительные образцы метаданных из внешних источников в рамках системы обратной связи ESET LiveGrid®, благодаря которой ESET может мгновенно реагировать на нужды пользователей и своевременно адаптироваться под новейшие угрозы. Мы рассчитываем на то, что вы будете присылать нам:
  - зараженные элементы, такие как потенциальные образцы вирусов и прочих вредоносных программ; подозрительные, проблемные, потенциально нежелательные и небезопасные объекты, такие как исполняемые файлы, сообщения электронной почты, про которые сообщили вы как про спам или которые выявил наш продукт;
  - информацию об устройствах в локальной сети, например тип, производитель, модель и/или название;
  - сведения о пользовании Интернетом, например IP-адрес, географическое расположение, пакеты IP, URL-адреса и кадры Ethernet;
  - файлы аварийных дампов и их содержимое.

Мы не стремимся собирать какие-либо данные, кроме обозначенных выше, но иногда этого невозможно избежать. Случайно собранные данные могут входить в состав вредоносных программ (будучи собранными без вашего ведома и одобрения) либо входить в имена файлов и URL-адреса, и Мы не намерены делать их частью наших систем или обрабатывать их для целей, указанных в настоящей Политике конфиденциальности.

- Сведения о лицензиях, например идентификаторы лицензий, и личные данные, например имя, фамилия, адрес, электронная почта, необходимые для выставления счетов, проверки

подлинности лицензий и предоставления наших услуг.

- Для обслуживания и предоставления поддержки может потребоваться контактная информация и данные, указанные в Ваших запросах на поддержку. Исходя из выбранного способа общения, Мы можем фиксировать Ваш электронный адрес, номер телефона, информацию о лицензии, сведения о программах и описание Вашего инцидента. Возможно, служба поддержки попросит Вас предоставить дополнительную информацию, чтобы упростить решение проблемы.

Конфиденциальность данных

ESET — это международная компания. Наша сеть распространения, обслуживания и поддержки состоит из аффилированных лиц и партнеров. Мы можем обмениваться информацией, которую обрабатывает ESET, с аффилированными лицами для выполнения соглашений EULA, например для предоставления поддержки или выставления счетов. В зависимости от Вашего расположения и выбранной услуги Нам, возможно, потребуется передать Ваши данные в страну, в которой не действуют нормативы Европейской Комиссии. Даже в этом случае сведения передаются лишь при необходимости и в соответствии с законодательством в сфере защиты данных. Во всех случаях без исключения должны применяться стандартные контрактные условия, обязательные корпоративные правила или другие соответствующие средства защиты.

Мы стремимся хранить данные не дольше, чем это необходимо для предоставления услуг в соответствии с Лицензионным соглашением. Длительность нашего периода хранения может превышать срок действия вашей лицензии — это дает Вам возможность простого и удобного продления. Сведенная к минимуму и анонимизированная статистика, а также прочие данные системы ESET LiveGrid® могут в дальнейшем обрабатываться в статистических целях.

ESET проводит соответствующие технические и организационные мероприятия, чтобы гарантировать уровень безопасности согласно возможным рискам. Мы делаем все возможное для непрерывного обеспечения конфиденциальности, целостности, доступности и устойчивости систем и служб обработки. Однако, если произойдет утечка данных, которая будет угрожать Вашим правам и свободам, Мы готовы уведомить органы по надзору, а также субъекты данных. Как субъект данных Вы имеете право подать жалобу в наблюдательный орган.

Права субъекта данных

ESET действует согласно словацким законам и законам о защите данных ЕС. Согласно условиям, которые определены действующим законодательством по защите данных, Вы как субъект данных имеете следующие права:

- запросить доступ к своим персональным данным, которыми располагает ESET;
- запросить исправление неточных данных (у Вас также есть право на дополнение неполных данных);
- запросить уничтожение своих персональных данных;
- запросить ограничение обработки своих персональных данных;
- право на запрет обработки данных;

- право на подачу жалобы, а также
- запросить переносимость данных.

Если Вы хотите воспользоваться своими правами субъекта данных или у Вас возникнет вопрос или проблема, отправьте нам письмо по адресу:

ESET, spol. s r.o.
Data Protection Officer
Einsteinova 24
85101 Bratislava
Slovak Republic
dpo@eset.sk