ESET Cyber Security Pro

Руководство пользователя

Щелкните здесь чтобы отобразить этого документа (онлайн-справка)

Авторское право ©2023 ESET, spol. s r.o.

ESET Cyber Security Pro разработано компанией ESET, spol. s r.o.

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

Все права защищены. Ни одна часть этой документации не может воспроизводиться, храниться в системе получения и передаваться в любой форме или любыми средствами, в том числе электронными и механическими способами, с помощью фотокопирования, записи, сканирования, а также любыми другими способами без письменного разрешения автора.

ESET, spol. s r.o. оставляет за собой право изменять любое описанное прикладное программное обеспечение без предварительного уведомления.

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

ПРОВ. 19.03.2023

1 ESET Cyber Security Pro 1
1.1 Новые возможности версии 6 1
1.2 Системные требования 1
2 Установка 2
2.1 Обычная установка 3
2.2 Выборочная установка 4
2.3 Разрешение расширений системы 5
2.4 Разрешение полного доступа к диску 6
3 Активация программы 7
4 Удаление программы 7
5 Основные сведения 7
5.1 Сочетания клавиш 8
5.2 Проверка состояния защиты 8
5.3 Действия, которые следует выполнить, если программа не работает надлежащим образом 9
6 Защита компьютера 9
6.1 Защита от вирусов и шпионских программ 10
6.1 Общие 10
6.1 Исключения 10
6.1 Защита при запуске 11
6.1 Защита файловой системы в режиме реального времени 11
6.1 Расширенные параметры 12
6.1 Изменение конфигурации защиты в режиме реального времени 12
6.1 Проверка защиты в режиме реального времени 13
6.1 Действия, которые следует выполнить, если модуль защиты в режиме реального времени не работает 13
6.1 Сканирование компьютера по требованию 13
6.1 Тип сканирования 14
6.1 Сканирование Smart 14
6.1 Выборочное сканирование 15
6.1 Объекты сканирования 15
6.1 Профили сканирования 15
6.1 Настройка параметров модуля ThreatSense 16
6.1 Объекты 17
6.1 Параметры 18
6.1 Очистка 18
6.1 Исключения 19
6.1 Ограничения 19
6.1 Другие 19
6.1 Действия при обнаружении заражения 20
6.2 Сканирование и блокирование съемных носителей 21
7 Защита от фишинга 22
8 Файервол 22
8.1 Режимы фильтрации 22
8.2 Правила для файервола 23
8.2 Создание новых правил 24
8.3 Зоны файервола 24
8.4 Профили файервола 24
8.5 Журналы файервола 25
9 Защита доступа в Интернет и электронной почты 25
9.1 Защита доступа в Интернет 26
9.1 Порты 26

9.1 Списки URL-адресов ... 26
9.2 Защита электронной почты ... 26
9.2 Проверка протокола POP3 ... 27
9.2 Проверка протокола IMAP ... 28
10 Родительский контроль ... 28
11 Обновление ... 29
11.1 Настройка обновления ... 29
11.1 Расширенные параметры ... 29
11.2 Создание задач обновления ... 30
11.3 Обновление ESET Cyber Security Pro до новой версии ... 30
11.4 Обновления системы ... 31
12 Сервис ... 32
12.1 Файлы журнала ... 32
12.1 Обслуживание журнала ... 32
12.1 Фильтрация журнала ... 33
12.2 Планировщик ... 34
12.2 Создание задач ... 35
12.2 Сканирование от имени владельца каталога ... 36
12.2 Создание пользовательских задач ... 36
12.3 Карантин ... 37
12.3 Помещение файлов на карантин ... 37
12.3 Восстановление из карантина ... 38
12.3 Отправка файла из карантина ... 38
12.4 Запущенные процессы ... 38
12.5 Сетевые подключения ... 39
12.6 Live Grid ... 39
12.6 Настройка Live Grid ... 40
12.7 Отправка образца на анализ ... 41
13 Интерфейс ... 41
13.1 Предупреждения и уведомления ... 42
13.1 Отображение предупреждений ... 42
13.1 Состояния защиты ... 43
13.2 Разрешения ... 43
13.3 Контекстное меню ... 44
13.4 Импорт и экспорт параметров ... 45
13.5 Настройка прокси-сервера ... 45
14 Лицензионное соглашение с конечным пользователем ... 46
15 Политика конфиденциальности ... 54

ESET Cyber Security Pro

ESET Cyber Security Pro представляет собой новый подход к по-настоящему интегрированному обеспечению безопасности компьютера. Последняя версия модуля сканирования ThreatSense® в сочетании с защитой клиента электронной почты, файерволом и родительским контролем характеризуется скоростью и точностью при обеспечении безопасности компьютера. Результатом является интеллектуальная система, которая постоянно защищает компьютер от атак и вредоносного программного обеспечения.

ESET Cyber Security Pro — это комплексное решение для обеспечения безопасности, созданное благодаря нашим долгосрочным усилиям и сочетающее максимальную защиту с минимальным влиянием на работу системы. Передовые технологии, основанные на искусственном интеллекте, которые используются в ESET Cyber Security Pro, способны обеспечить упреждающую защиту от вирусов, червей, троянских, шпионских и рекламных программ, руткитов и прочих интернет-атак, не ухудшая производительность системы.

Новые возможности версии 6

В версии 6 программы ESET Cyber Security Pro представлены следующие обновления и улучшения.

- **Поддержка 64-разрядной архитектуры**
- **Защита от фишинга**. Данная функция предотвращает получение ваших личных данных поддельными веб-сайтами, которые выдают себя за надежные.
- **Обновления системы**. Версия 6 программы ESET Cyber Security Pro включает в себя различные исправления и улучшения, в том числе уведомления об обновлениях операционной системы. Чтобы узнать подробнее, см. раздел Обновления системы.
- **Состояния защиты**. Этот параметр скрывает уведомления с экрана состояния защиты (например, Защита электронной почты отключена или Требуется перезапуск компьютера).
- **Носители для сканирования**. Определенные типы носителей можно исключать из сканирования в режиме реального времени (локальные диски, съемные носители, сетевые носители).
- **Сетевые подключения**. Этот параметр отображает сетевые подключения вашего компьютера и дает возможность создавать правила для таких подключений.

Для получения дополнительной информации о новых функциях ESET Cyber Security Pro прочитайте следующую статью базы знаний ESET:

Требования к системе

Для оптимальной работы ESET Cyber Security Pro система должна соответствовать указанным ниже требованиям к оборудованию и программному обеспечению.

	Системные требования:
Архитектура процессора	Intel 64-bit, M1, M2

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 решение ESET Cyber Security Pro 6.10.900.0 и более поздних версий поддерживает процессоры Apple M1 и M2 при условии использования Rosetta 2.

Установка

Прежде чем приступать к процессу установки, нужно закрыть все открытые на компьютере программы. ESET Cyber Security Pro содержит компоненты, которые могут конфликтовать с другими установленными на компьютере программами защиты от вирусов. ESET настоятельно рекомендует удалить любые другие программы защиты от вирусов, чтобы предотвратить возможные проблемы.

Для запуска мастера установки выполните одно из перечисленных далее действий.

- Если установка выполняется с помощью файла, загруженного с веб-сайта ESET, откройте его и дважды щелкните значок **Установить**.
- Если установка выполняется с компакт- или DVD-диска, вставьте его в дисковод, откройте на рабочем столе или в окне **Finder** и дважды щелкните значок **Установить**.



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

После принятия условий лицензионного соглашения вы сможете выбрать один из указанных ниже типов установки.

- Обычная установка

- Выборочная установка

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 Cyber Security Pro:

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 Cyber Security Pro **хочет добавить конфигурации прокси-сервера**. 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 Cyber Security Pro отобразит уведомление о том, что **компьютер не защищен**. Чтобы получить доступ ко всем функциям ESET Cyber Security Pro, 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 Cyber Security Pro о том, что **ваш компьютер защищен частично**. Чтобы получить доступ ко всем функциям ESET Cyber Security Pro, необходимо разрешить **полный доступ к диску** для программы ESET Cyber Security Pro. 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 Cyber Security Pro.

На компьютере отобразится уведомление о необходимости перезагрузить систему. Щелкните **Позже**. Пока не перезагружайте компьютер. Щелкните **Начать заново** в окне уведомления программы ESET Cyber Security Pro или перезагрузите компьютер. Более подробные сведения см. в статье нашей базы знаний.

После установки ESET Cyber Security Pro 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.

• **Прокси-сервер**
Если вы используете прокси-сервер, укажите его параметры, установив флажок **Я использую прокси-сервер**. Далее введите IP-адрес или URL-адрес прокси-сервера в поле **Адрес**. В поле **Порт** укажите порт, по которому этот прокси-сервер принимает запросы на подключение (по умолчанию 3128). Если прокси-сервер требует аутентификации, введите правильные **имя пользователя** и **пароль**, которые необходимы для доступа к нему. Если вы не используете прокси-сервер, выберите вариант**Я не использую прокси-сервер**. Если вы не знаете точно, используется ли прокси-сервер, выберите **Использовать системные параметры (рекомендуется)**, чтобы использовать текущие системные параметры.

• **Разрешения**
Можно определить особых пользователей или группы пользователей, которые получат разрешения на изменение конфигурации программы. Выберите их в списке в левой части окна и нажмите кнопку **Добавить**, чтобы добавить их в список **Пользователи с правами**. Чтобы отобразить всех системных пользователей, установите флажок **Показывать всех пользователей**. Если список "Пользователи с правами" пуст, все пользователи рассматриваются как обладатели прав.

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

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

• **файервол;**
Для файервола можно выбрать режим фильтрации. Дополнительные сведения см. в разделе Режимы фильтрации.После установки ESET Cyber Security Pro:

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 Cyber Security Pro **хочет добавить конфигурации прокси-сервера**. 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 Cyber Security Pro отобразит уведомление о том, что **компьютер не защищен**. Чтобы получить доступ ко всем функциям ESET Cyber Security Pro, 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 Cyber Security Pro о том, что **ваш компьютер защищен частично**. Чтобы получить доступ ко всем функциям ESET Cyber Security Pro, необходимо разрешить **полный доступ к диску** для программы ESET Cyber Security Pro. 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 Cyber Security Pro. На компьютере отобразится уведомление о необходимости перезагрузить систему. Щелкните **Позже**. Пока не перезагружайте компьютер. Щелкните **Начать заново** в окне уведомления программы ESET Cyber Security Pro или перезагрузите компьютер. Более подробные сведения см. в статье нашей базы знаний.

После установки ESET Cyber Security Pro 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

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

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



Обновление с предыдущей версии macOS до Big Sur
Если вы уже установили ESET Cyber Security Pro 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 обе опции ESET Cyber Security Pro**.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

В системе macOS 10.14 вы получите уведомление от программы ESET Cyber Security Pro о том, что **ваш компьютер защищен частично**. Для доступа ко всем функциям ESET Cyber Security Pro необходимо разрешить программе ESET Cyber Security Pro **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 Cyber Security Pro**.app** из списка.
5. Отобразится уведомление о перезапуске ESET Cyber Security Pro. 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 Cyber Security Pro или перезапустите компьютер. Более подробные сведения см. в статье нашей базы знаний.

Активация продукта

После установки окно активации продукта отобразится автоматически. Чтобы открыть диалоговое окно активации продукта в любое время, щелкните значок ESET Cyber Security Pro, расположенный в строке меню macOS (в верхней части экрана), и выберите пункт **Активация продукта...**.

• **Лицензионный ключ**: уникальная строка в формате XXXX-XXXX-XXXX-XXXX-XXXX или XXXX-XXXXXXXX, которая используется для идентификации владельца лицензии и ее активации. Если вы приобрели розничную упакованную версию продукта, активируйте ее с помощью лицензионного ключа. Обычно его можно найти внутри упаковки программного продукта или на ее тыльной стороне.

• **Имя пользователя и пароль**: если у вас есть имя пользователя и пароль и вы не знаете, как активировать ESET Cyber Security Pro, щелкните **У меня есть имя пользователя и пароль. Что мне делать?**. Откроется сайт my.eset.com, где можно будет получить лицензионный ключ на основании учетных данных.

• **Пробная лицензия**: выберите этот параметр, если хотите ознакомиться с программой ESET Cyber Security Pro до покупки. Укажите свой адрес электронной почты, чтобы активировать ESET Cyber Security Pro на ограниченный период времени. Тестовая лицензия будет отправлена вам по электронной почте. Каждый пользователь может активировать только одну пробную лицензию.

• **Приобрести лицензию**: если у вас нет лицензии, но вы хотите купить ее, выберите вариант «Приобрести лицензию». В результате откроется веб-сайт местного распространителя ESET.

• **Активировать позже**: выберите этот вариант, если активация в данный момент не требуется.

Удаление программы

Чтобы удалить ESET Cyber Security Pro, выберите один из вариантов.

• Вставьте установочный компакт- или DVD-диск с программой ESET Cyber Security Pro в дисковод, откройте его на рабочем столе или в окне **Finder** и дважды щелкните **Удалить**.

• Откройте установочный файл ESET Cyber Security Pro (*DMG*-файл) и дважды щелкните **Удалить**.

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

Основные сведения

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

В главном меню можно получить доступ к следующим разделам.

• **Домашняя страница**: отображается информация о состоянии защиты компьютера, доступа в Интернет и электронной почты, а также о состоянии файервола и родительского контроля.

• **Сканирование компьютера**: этот раздел позволяет настроить и запустить сканирование компьютера по требованию.

• **Обновление**: отображение информации об обновлении модулей обнаружения.

• **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 Cyber Security Pro.

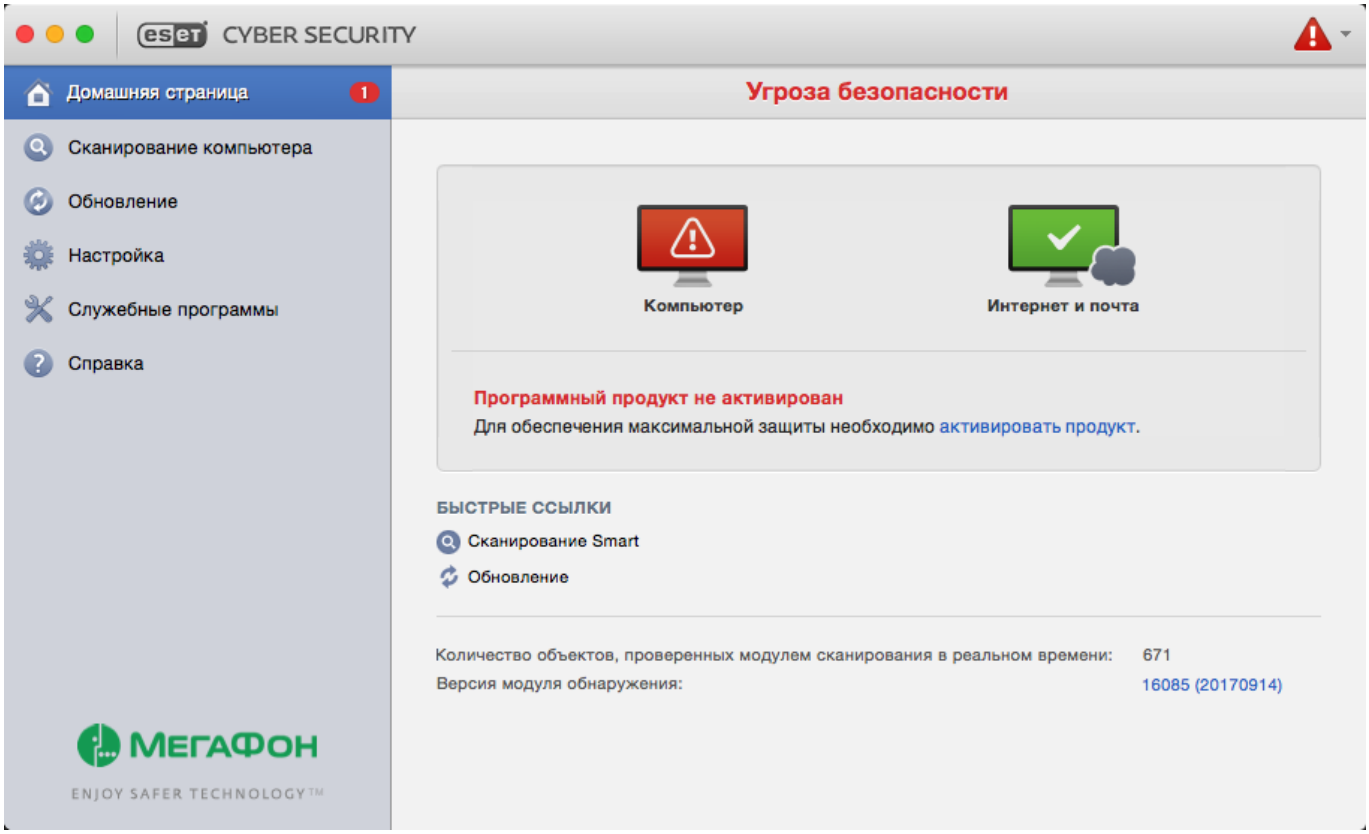
- cmd+,: отображает настройки ESET Cyber Security Pro.
- cmd+O — восстановление размера по умолчанию главного окна программы ESET Cyber Security Pro и его перемещение в центр экрана.
- cmd+Q: позволяет скрыть главное окно графического интерфейса программы ESET Cyber Security Pro. Его можно открыть, щелкнув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

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 состояния защиты

Чтобы просмотреть состояние защиты, в главном меню откройте вкладку **Домашняя страница**. В основном окне появится сводная информация о работе модулей ESET Cyber Security Pro.



Действия, которые следует выполнить, если программа не работает надлежащим образом

Если модуль работает должным образом, отображается зеленый значок. Если модуль работает ненадлежащим образом, отобразится красный восклицательный знак или оранжевый значок оповещения. Отображаются дополнительные сведения об этом модуле и предлагается решение для устранения проблемы. Чтобы изменить состояние отдельных модулей, щелкните синюю ссылку внизу каждого уведомления.

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

Защита компьютера

Конфигурацию компьютера можно найти, выбрав **Настройка** > **Компьютер**. Отобразятся данные о состоянии **защиты файловой системы в режиме реального времени** и **блокирования съемных носителей**. Для отключения отдельных модулей следует переключить кнопку соответствующего модуля в положение **ОТКЛЮЧЕНО**. Обратите внимание, что это может понизить уровень защиты компьютера. Для доступа к детальным настройкам каждого модуля 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**. Потенциально нежелательные приложения представляют собой довольно широкую категорию программного обеспечения, задачей которого не является однозначно вредоносная деятельность в отличие от других типов вредоносных программ, таких как вирусы или троянские программы. Однако такое приложение может устанавливать дополнительное нежелательное программное обеспечение, изменять поведение цифрового устройства, а также выполнять действия без запроса или разрешения пользователя. Дополнительную информацию о приложениях этого типа см. в глоссарии.

• **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 используются злоумышленниками, чтобы избежать обнаружения. Упаковщик — это самораспаковывающийся исполняемый файл среды выполнения, который позволяет добавить несколько типов вредоносного ПО в один пакет. Наиболее распространенными упаковщиками являются UPX, PE_Compact, PKLite и ASPack. Одно и то же вредоносное ПО может обнаруживаться по-разному при сжатии разными упаковщиками. Также у упаковщиков есть способность с течением времени изменять свои «подписи», 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 запуска, 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 ее 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**: отмена всех исключений.

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

Защита при запуске

Функция проверки файлов, исполняемых при запуске системы, предусматривает автоматическое сканирование файлов во время запуска системы. По умолчанию такое сканирование выполняется регулярно как запланированная задача после входа пользователя в систему и после успешного обновления модулей обнаружения. Чтобы изменить параметры модуля ThreatSense, применимые к сканированию при запуске системы, нажмите кнопку **Настройка**. Дополнительные сведения о настройке модуля ThreatSense приведены в этом разделе.

Защита файловой системы в режиме реального времени

Защита файловой системы в режиме реального времени проверяет все типы носителей и запускает сканирование при различных событиях. 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 возможен более точный контроль.

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 Cyber Security Pro, 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**).

Следующие типы носителей можно исключить из модуля сканирования Real-time:

• **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 ThreatSense для исполняемых файлов — по умолчанию при исполнении файлов используется **расширенная эвристика**. Настоятельно рекомендуется не выключать функцию оптимизации Smart и систему ESET Live Grid, чтобы уменьшить воздействие на работу компьютера.

Повысить совместимость сетевых томов — этот параметр повышает производительность компьютера при открытии файлов по сети. Его следует включать, если работа компьютера замедляется при работе с сетевыми дисками. Эта функция использует координатор файлов в macOS 10.10 и более поздних версиях. Обратите внимание, что не все приложения поддерживают координатор файлов, например Microsoft Word 2011 не поддерживает его, а Word 2016 поддерживает.

Изменение конфигурации защиты в режиме реального времени

Функция защиты в режиме реального времени является наиболее важным элементом всей системы обеспечения безопасности ESET Cyber Security Pro. Изменять параметры модуля защиты в режиме реального времени следует с осторожностью. Рекомендуется делать это только в особых случаях, например в ситуации, когда существует конфликт с определенным приложением.

После установки ESET Cyber Security Pro все параметры оптимизированы для максимальной защиты системы. Чтобы восстановить параметры по умолчанию, нажмите кнопку **По умолчанию** в левом нижнем углу окна **Защита в режиме реального времени** (**Настройка** > **Настроить параметры приложения...** > **Защита в режиме реального времени**).

Проверка защиты в режиме реального времени

Чтобы убедиться в том, что функция защиты в режиме реального времени работает и обнаруживает вирусы, загрузите тестовый файл с сайта eicar.com и проверьте, опознает ли ESET Cyber Security Pro его как угрозу. Это специальный безвредный файл, обнаруживаемый всеми программами защиты от вирусов. Он создан институтом EICAR (Европейский институт антивирусных компьютерных исследований) для тестирования функциональности программ защиты от вирусов.

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

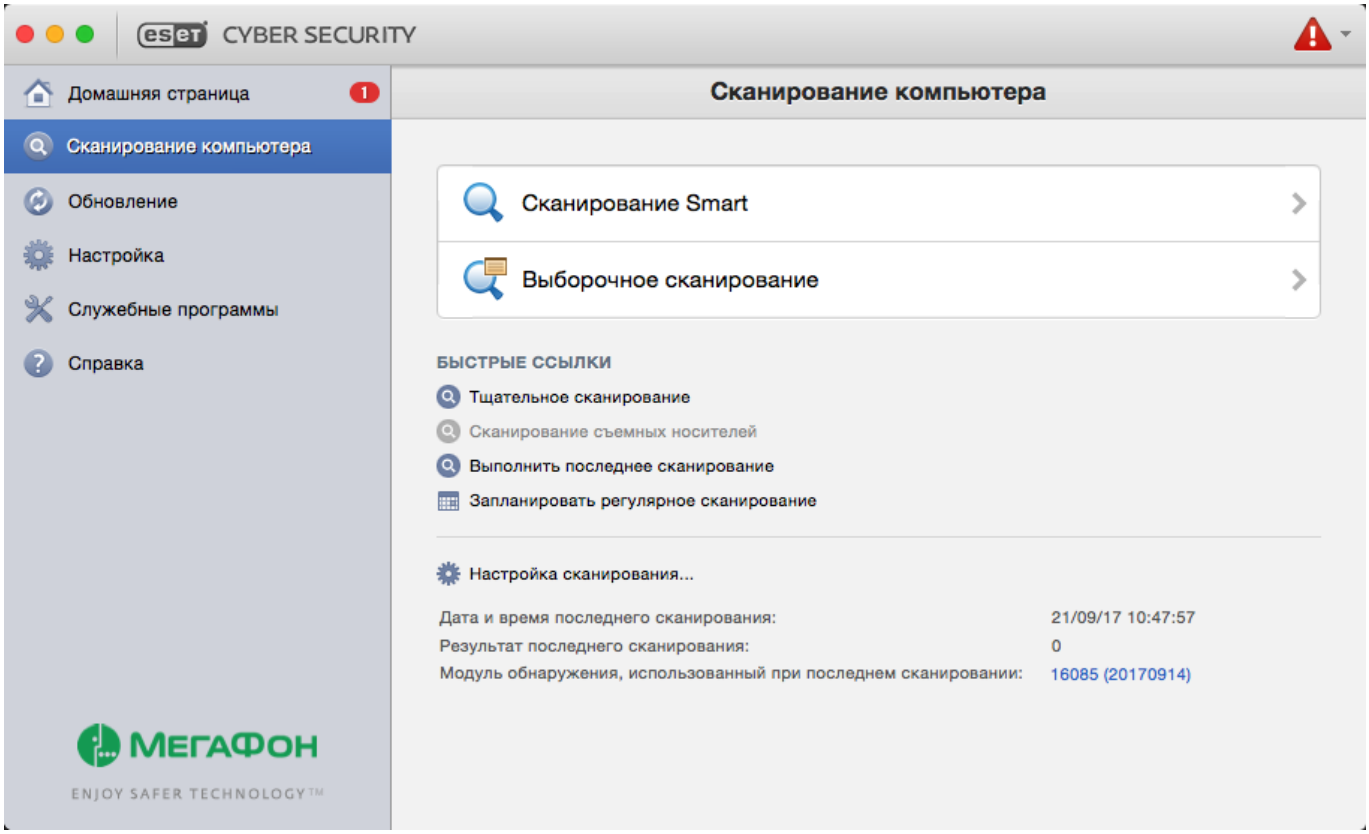
Если защита в режиме реального времени не инициализируется при запуске системы, это может быть вызвано конфликтом с другими программами. В этом случае обратитесь в службу технической поддержки ESET.

Сканирование ПК 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 заражения, не обнаруженные модулем сканирования в режиме реального времени при их записи на диск. Это может произойти, если модуль сканирования в режиме реального времени был отключен во время заражения или использовались устаревшие модули обнаружения.

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



Тип сканирования

Доступны два типа сканирования компьютера по требованию. **Сканирование Smart** позволяет быстро просканировать систему без настройки каких-либо параметров. Тип **Выборочное сканирование** позволяет выбрать предопределенный профиль сканирования, а также указать конкретные объекты.

Сканирование Smart

Сканирование Smart позволяет быстро запустить сканирование ПК и очистить зараженные файлы без вмешательства пользователя. Главным преимуществом этого метода является простота использования без детальной настройки параметров 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 является оптимальным решением в том случае, если нужно указать параметры сканирования (например, объекты и методы сканирования). Преимуществом такого сканирования выступает возможность детальной настройки параметров. Различные конфигурации можно сохранить в виде пользовательских профилей сканирования, которые полезны при регулярном сканировании с одинаковыми параметрами.

Чтобы указать объекты сканирования, последовательно выберите элементы **Сканирование компьютера** > **Выборочное сканирование** и отметьте в древовидной структуре нужные объекты. Объекты сканирования также можно задать более точно, указав пути к папкам и файлам, которые нужно сканировать. Если нужно только выполнить сканирование системы 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

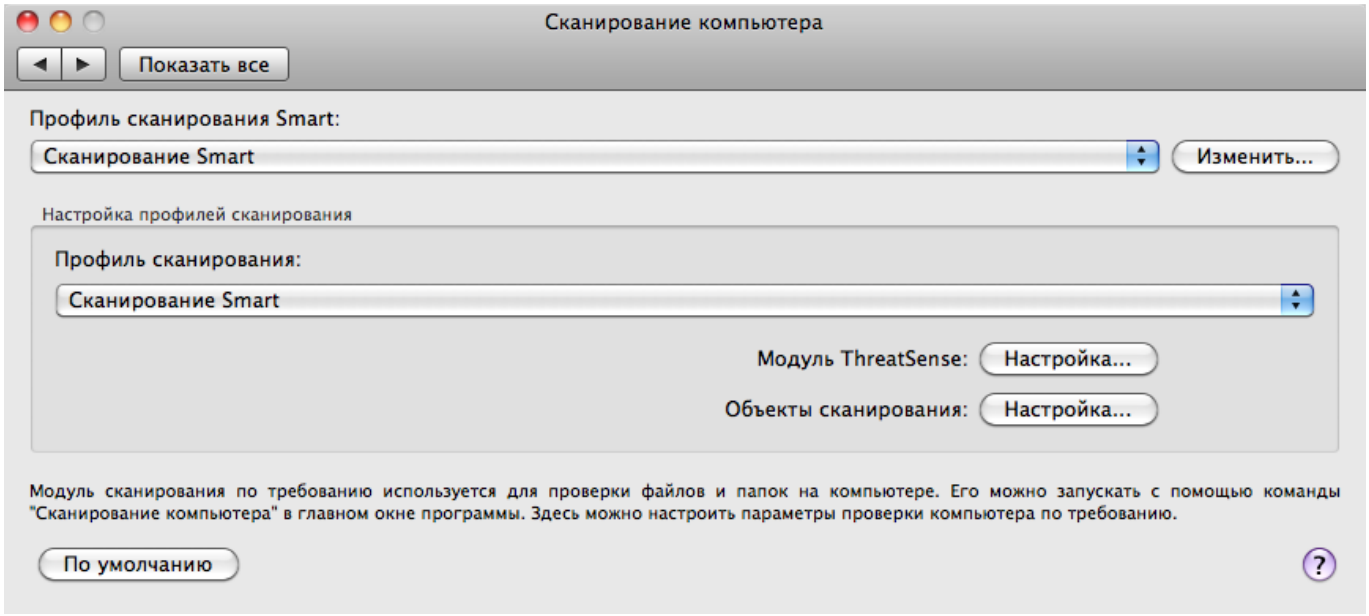
Древовидная структура объектов сканирования позволяет выбрать файлы и папки, которые необходимо просканировать на наличие вирусов. Выбор папок может также осуществляться в соответствии с параметрами профиля.

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 флажок возле соответствующего файла или папки.

Профили сканирования

Предпочтительные настройки сканирования можно сохранить для использования в будущем. Рекомендуется создать отдельный профиль для каждого регулярно используемого сканирования (с различными объектами, методами сканирования и прочими параметрами).

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...**.



Информацию о создании профиля, соответствующего конкретным требованиям, и описание настройки для каждого параметра сканирования см. в разделе Настройка параметров модуля ThreatSense.

Пример. Предположим, пользователю необходимо создать собственный профиль сканирования, и конфигурация сканирования Smart частично устраивает его, при этом ему не требуется сканировать упаковщики и потенциально опасные приложения, но нужно применить тщательную очистку. В диалоговом окне **Список профилей модуля сканирования по требованию** введите имя профиля и нажмите кнопку **Добавить**, а затем — **ОК**. После этого задайте необходимые параметры, настроив **модуль ThreatSense** и указав **объекты сканирования**.

Если вы хотите, чтобы по завершении сканирования операционная система была отключена, а компьютер выключен, воспользуйтесь параметром **Завершить работу компьютера после сканирования**.

Настройка параметров модуля ThreatSense

ThreatSense — это проприетарная технология компании ESET, включающая в себя несколько сложных методов обнаружения угроз. Эта технология является упреждающей, т. е. она защищает от новой угрозы уже в первые часы ее распространения. 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 максимально повышается эффективность обнаружения. Также технология ThreatSense эффективно предотвращает проникновение руткитов.

Параметры настройки технологии ThreatSense позволяют указать несколько параметров сканирования:

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

Чтобы открыть окно параметров, последовательно выберите элементы **Настройка > Дополнительные настройки** (или нажмите *cmd+,*), а затем нажмите кнопку **Настройка** модуля ThreatSense, расположенную в модулях **Защита при запуске**, **Защита в режиме реального времени** и **Сканирование компьютера**, каждый из которых использует технологию ThreatSense (см. ниже). Для разных сценариев обеспечения безопасности могут требоваться различные конфигурации, поэтому параметры модуля ThreatSense можно настроить отдельно для каждого из следующих модулей защиты.

- **Защита при запуске** — автоматическая проверка файлов, исполняемых 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 проверить 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 последующих действий предоставляется и в том случае, если предопределенное 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.



Архивные файлы

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.



Сканирование 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. Любое расширение можно добавить в список исключений из сканирования. С помощью кнопок  и  можно включить или запретить сканирование определенных 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 степень вложенности архивов для сканирования.

• **Максимальный размер:** определяет максимальный размер сканируемых объектов. После указания максимального размера модуль защиты от вирусов будет проверять только объекты меньше указанного размера. Этот параметр 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 времени независимо от того, завершено ли оно.

• **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:** позволяет задать максимальный размер файлов в архивах (после извлечения), подлежащих сканированию. Если из-за этого ограничения сканирование преждевременно прерывается, 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 Cyber Security Pro 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 используемые файловой системой — это связи файлов и папок, недоступные для обычных методик сканирования. Многие вредоносные программы выдают себя за альтернативные потоки данных, чтобы не быть обнаруженными.

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.).

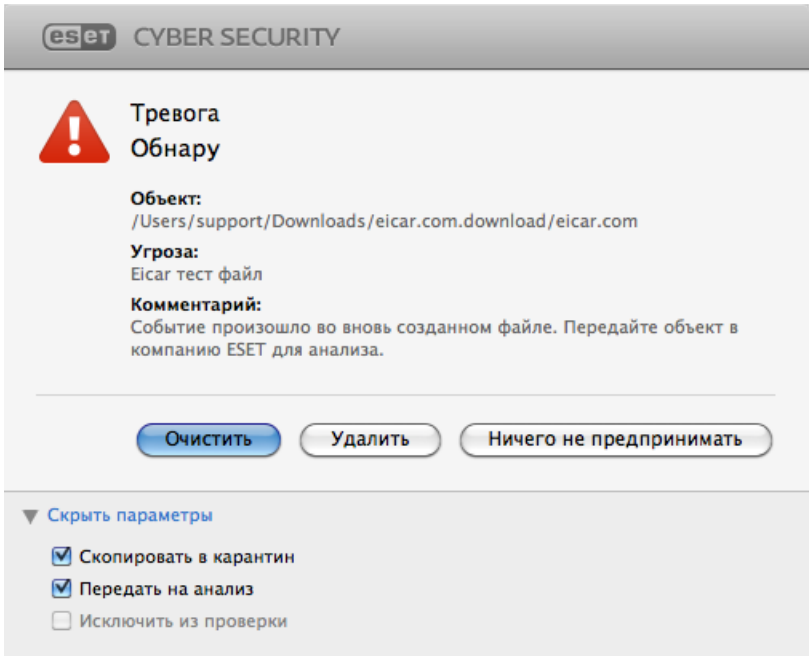
Если наблюдаются признаки заражения компьютера (например, он стал медленнее работать, часто «зависает» и т. п.), рекомендуется выполнить действия, описанные ниже.

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 следует сканировать только определенную часть диска, выберите вариант **Выборочное сканирование** и укажите объекты, которые нужно сканировать на наличие вирусов.

Ниже описано, что происходит, когда ESET Cyber Security Pro выявляет заражение. Предположим, что заражение обнаружено модулем защиты файловой системы в режиме реального времени при используемом по умолчанию уровне очистки. Сначала модуль защиты в режиме реального времени пытается очистить или удалить файл. Если действие по умолчанию для модуля защиты в режиме реального времени не определено, его предлагается выбрать пользователю. Обычно можно выбрать действие **Очистить**, **Удалить** или **Ничего не предпринимать**. Действие **Ничего не предпринимать** выбирать не рекомендуется, так как в этом случае зараженный файл останется в зараженном состоянии. Этот параметр предназначен для ситуаций, когда имеется полная уверенность в том, 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.



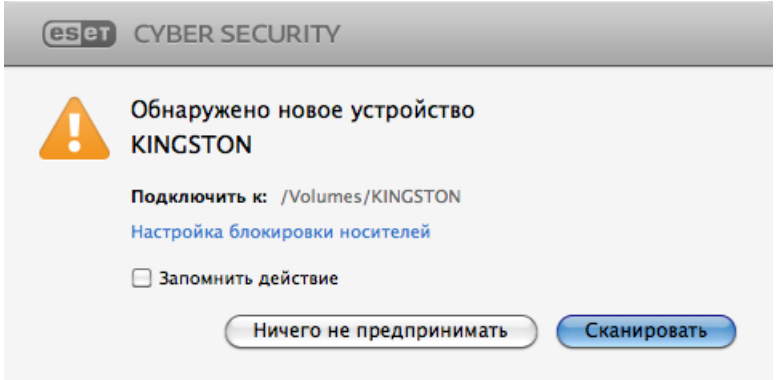
Удаление файлов из архивов.
В режиме очистки по умолчанию архив удаляется целиком только в случае, если он содержит только зараженные файлы. Иначе говоря, архивы, в которых есть незараженные файлы, не удаляются. Однако сканирование в режиме **Тщательная очистка** следует применять с осторожностью: в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

Сканирование и блокирование съемных носителей

Программа ESET Cyber Security Pro дает возможность выполнять по требованию сканирование вставленных в компьютер съемных накопителей (компакт- и DVD-дисков, USB-устройств и т. д.). В macOS 10.15 программа ESET Cyber Security Pro может сканировать и другие внешние носители.

Сканирование съемных носителей в macOS 11 и более поздних версиях

Программа ESET Cyber Security Pro, установленная в macOS 11 и более поздних версиях, сканирует только накопители.



Съемные носители могут содержать вредоносный код и подвергать компьютер риску. Чтобы

заблокировать съемный носитель, щелкните элемент **Настройка блокировки носителей** (см. изображение выше) или в главном меню последовательно выберите элементы **Настройка** > **Задать настройки приложения** > **Носитель** и установите флажок **Включить блокирование съемных носителей**. Чтобы разрешить доступ к носителям определенного типа, снимите соответствующие флажки.



Доступ к компакт-диску

Чтобы разрешить доступ к внешнему устройству чтения компакт-дисков, которое подключено к компьютеру при помощи USB-кабеля, снимите флажок **Компакт-диск**.

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 Cyber Security Pro 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 для параметра **Блокировать весь сетевой трафик: отключить сеть** установить значение **ВКЛЮЧЕНО**, все входящие и исходящие соединения будут блокироваться файерволом. Используйте этот параметр только в особых случаях, когда возникает опасная критическая ситуация, требующая немедленного отключения системы от сети.

Режимы фильтрации

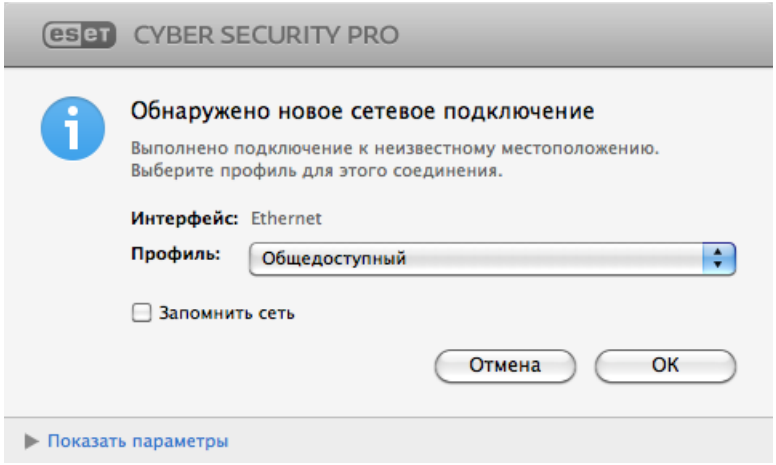
В файерволе ESET Cyber Security Pro есть три режима фильтрации. Параметры режимов фильтрации можно найти в настройках программы ESET Cyber Security Pro (нажмите *cmd+,*) >

Файервол. Поведение файервола меняется в зависимости от выбранного режима. Режимы фильтрации влияют также на необходимый уровень вмешательства пользователя.

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 пользовательскую конфигурацию файервола. При обнаружении соединения, к которому не применяются существующие правила, отображается диалоговое окно с сообщением о неизвестном подключении. В диалоговом окне можно разрешить или запретить соединение, и этот выбор может быть сохранен как новое правило для файервола. Если вы решите создать новое правило, все будущие подключения данного типа будут разрешены или заблокированы в соответствии с правилом.



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 **Сервис** > **Журналы** и в раскрывающемся меню **Журнал** выберите пункт **Файервол**.

Правила файервола

Правила файервола представляют собой набор условий, которые позволяют проверять все сетевые подключения и определяют соответствующие действия для этих условий. В правилах 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 подключении все наоборот — 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.

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

Создание правил

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

1. Чтобы создать новое правило, щелкните **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 параметр **Все приложения**.

2. В следующем окне необходимо указать **действие** (разрешить или запретить обмен данными между выбранным приложением и сетью) и **направление** соединения (входящее, исходящее или оба направления). Можно записать в файл журнала все соединения, которые относятся к данному правилу. Для этого выберите параметр **Правило журнала**. Для просмотра журналов в главном меню ESET Cyber Security Pro выберите пункт **Сервис** > **Журналы** и в раскрывающемся меню **Журнал** выберите пункт **Файервол**.

3. В разделе **Протокол/порты** выберите протокол, который используется для приложения, и номера портов (если выбран протокол TCP или UDP). На уровне транспортного протокола обеспечивается безопасная и эффективная передача данных.

4. Наконец, укажите критерии **назначения** (IP-адрес, диапазон, подсеть, сеть Ethernet или Интернет) для правила.

Зоны файервола

Зона представляет собой набор сетевых адресов, которые составляют одну логическую группу. Каждому адресу в группе присваивается аналогичное правило, которое определено для всей группы в целом.

Эти зоны можно создать, нажав кнопку **Добавить...**. Введите для зоны **имя** и **описание** (необязательно), выберите профиль, к которому будет принадлежать данная зона, и добавьте адрес IPv4/IPv6, диапазон адресов, подсеть, сеть Wi-Fi или интерфейс.

Профили файервола

С помощью **профилей** можно контролировать поведение файервола ESET Cyber Security Pro. 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 Cyber Security Pro 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.

Защита доступа в Интернет и электронной почты

Чтобы открыть раздел «Защита доступа в Интернет и электронной почты», в главном меню выберите **Настройка** > **Интернет и электронная почта**. Здесь можно также получить доступ к подробным настройкам каждого модуля, щелкнув параметр **Настройка...**.

- **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.



Исключения при сканировании

ESET Cyber Security Pro не сканирует зашифрованные протоколы HTTPS, POP3S и IMAPS.

Защита доступа в Интернет

Функция защиты доступа в Интернет отслеживает обмен данными между веб-браузерами и удаленными серверами на предмет соответствия правилам 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 URL-адресам из списка **Разрешенный URL-адрес**, выберите параметр **Ограничить URL-адреса**.

Для активации списка выберите значение **Включено** рядом с именем списка. Если требуется уведомление при вводе адреса из текущего списка, установите флажок **С уведомлением**.

Во всех списках могут использоваться специальные символы *** (звездочка) и *?* (знак вопроса). Звездочка заменяет любую строку символов, а знак вопроса заменяет 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 обеспечивает контроль безопасности обмена данными по протоколам POP3 и IMAP. При проверке входящих сообщений ESET Cyber Security Pro использует все методы расширенного сканирования, которые обеспечивает модуль сканирования ThreatSense. Сканирование соединений по протоколам POP3 и IMAP не зависит от используемого почтового клиента.

Модуль **ThreatSense: Настройка**: расширенная настройка модуля сканирования позволяет выбирать объекты сканирования, методы обнаружения и т. д. Нажмите кнопку **Настройка**,

чтобы открыть окно расширенной настройки модуля сканирования.

Добавить уведомление к сообщениям электронной почты: после сканирования сообщения электронной почты можно добавить к нему уведомление, содержащее результаты сканирования. Уведомления являются полезным средством, однако их не следует воспринимать как гарантию безопасности сообщения, поскольку они могут затеряться в сложных сообщениях в формате HTML или быть сфабрикованы некоторыми угрозами. Доступны следующие варианты:

- **Никогда**: уведомления не добавляются к сообщениям электронной почты.
- **Только к зараженным сообщениям**: помечаются как проверенные только сообщения электронной почты, содержащие вредоносные программы.
- **Ко всем сканируемым сообщениям**: уведомления будут добавлены ко всем просканированным сообщениям электронной почты.

Добавлять примечание в поле темы полученных и прочитанных зараженных сообщений: установите этот флажок, если в тему зараженных сообщений необходимо добавлять предупреждения об угрозах, сгенерированные системой защиты электронной почты. Эта функция обеспечивает простоту фильтрации зараженных сообщений 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
- %aspmstatus%: изменяет тему в зависимости от результата сканирования на наличие спама
- %product%: добавляет название вашего продукта ESET (в данном случае — ESET Cyber Security Pro)
- %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 протоколам POP3 и IMAP. Подробные сведения об этом см. 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 Cyber Security Pro 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. Убедитесь, что модуль включен для надлежащей работы фильтрации протоколов. Проверка протокола POP3 осуществляется автоматически без необходимости повторной настройки клиента электронной почты. 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 для обнаружения вредоносных программ.

Проверка протокола IMAP

Протокол IMAP — это еще один интернет-протокол для получения электронной почты. У протокола IMAP есть определенные преимущества по сравнению с протоколом POP3. Например, к почтовому ящику могут одновременно подключаться несколько клиентов электронной почты и отображать актуальные данные о состоянии сообщения (было ли оно прочитано или нет, был ли дан на него ответ или было ли оно удалено). ESET Cyber Security Pro 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. Убедитесь, что для надлежащей работы модуля включена функция проверки протокола IMAP. Контроль протокола IMAP осуществляется автоматически без необходимости повторной настройки клиента электронной почты. 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 для обнаружения вредоносных программ.

Родительский контроль

В разделе **Родительский контроль** можно настроить параметры родительского контроля. Здесь представлены автоматизированные средства для защиты детей. Назначение этой функции — запретить детям и подросткам получать доступ к страницам с неприемлемым или опасным содержимым. Родительский контроль позволяет блокировать веб-страницы, которые могут содержать потенциально нежелательные материалы. Кроме того, родители могут запретить доступ к веб-сайтам из 27 предварительно созданных категорий.

Учетные записи пользователей перечислены в окне **Родительский контроль** (**Настройка** > **Дополнительные настройки** > **Родительский контроль**). Выберите учетную запись, в отношении которой необходимо осуществлять родительский контроль. Чтобы указать уровень защиты для выбранной учетной записи, щелкните **Настройка** . Чтобы создать новую учетную запись, щелкните **Добавить** . Откроется окно учетных записей системы macOS.

В окне **Настройка родительского контроля** в раскрывающемся меню **Настройка профиля** выберите один из предопределенных профилей или скопируйте настройку родительского контроля из другой учетной записи пользователя. Каждый профиль содержит измененный список разрешенных категорий. Если категория отмечена, значит она разрешена. Если навести курсор на определенную категорию, отобразится список веб-страниц, которые к ней относятся.

Чтобы изменить список **Разрешенные и заблокированные веб-страницы**, в нижней части окна щелкните **Настройка** и добавьте имя домена в нужный список. Не нужно вводить *http://*. Использовать символы подстановки (*) необязательно. Если ввести только имя домена, все

поддомены также будут включены. Например, если добавить *google.com* в **список разрешенных веб-страниц** все поддомены (*mail.google.com, news.google.com, maps.google.com* и т. д.) будут разрешены.

> **Правила**
> Блокирование или разрешение конкретной веб-страницы может быть более эффективным, чем блокирование или разрешение целой категории веб-страниц.

Обновление

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

Выберите пункт **Обновить** в главном меню, чтобы просмотреть информацию о текущем состоянии обновления ESET Cyber Security Pro, в том числе дату и время последнего успешно выполненного обновления, а также сведения о необходимости обновления. Чтобы начать процесс обновления вручную, щелкните **Обновление модулей**.

Обычно после корректного завершения загрузки в окне обновления выводится сообщение **Обновление не требуется — установлены актуальные версии модулей**. Если обновить модули невозможно, рекомендуется проверить настройки обновления, поскольку самая распространенная причина этой ошибки — неправильно введенные данные проверки подлинности (имя пользователя и пароль) или некорректно выбранные параметры подключения.

В окне обновления также указывается версия модуля обнаружения. Номер версии содержит ссылку на веб-страницу ESET, на которой указаны сведения об обновлении модуля обнаружения.

Настройка обновления

Чтобы удалить временные данные обновлений, нажмите кнопку **Очистить** рядом с пунктом **Очистить кэш обновлений**. Используйте эту функцию при возникновении проблем в ходе обновления.

Расширенные параметры

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

Чтобы загружать разрабатываемые модули на этапе финального тестирования, включите параметр **Обновление предварительной версии**. Обновления предварительной версии зачастую содержат исправления ошибок продукта. **Отложенное обновление**: загрузка обновлений спустя несколько часов после выпуска позволяет гарантировать, что клиенты получат их только после подтверждения отсутствия ошибок при работе в неэкспериментальной среде.

Программа ESET Cyber Security Pro создает снимки модулей обнаружения и модулей программы. Эти снимки используются с функцией **отката обновления**. Оставьте включенным параметр **Создавать снимки файлов обновлений**, чтобы программа ESET Cyber Security Pro записывала такие снимки автоматически. Если вы подозреваете, что последнее обновление модуля обнаружения и/или программного модуля повреждено или работает нестабильно, вы можете воспользоваться функцией отката до предыдущей версии и отключить обновления на установленный период времени. Чтобы откатить обновление до самой старой версии в истории, щелкните **Откат**. Кроме того, можно включить ранее отключенные обновления, если они были отложены на неопределенный период времени. В случае выполнения отката до предыдущей версии обновления воспользуйтесь раскрывающимся меню **Установить такой период приостановки** и укажите время, на которое требуется приостановить загрузку обновлений. При выборе варианта **До отзыва** обычное обновление не возобновится, пока вы его не включите вновь вручную. Чтобы вновь включить обновление вручную, щелкните **Разрешить**. Проявляйте осторожность, настраивая период приостановки для обновления.

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

Обновления можно запускать вручную. Для этого в главном меню щелкните элемент **Обновление**, а затем **Обновление модулей**.

Обновления также можно выполнять как запланированную задачу. Для конфигурирования запланированной задачи перейдите в раздел **Служебные программы** > **Планировщик**. По умолчанию в ESET Cyber Security Pro активированы указанные ниже задачи.

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

Каждую из задач обновления можно изменить в соответствии с конкретными требованиями. Кроме задач по умолчанию можно создать другие задачи обновления с пользовательскими настройками. Дополнительные сведения о создании и настройке задач обновления см. в разделе Планировщик.

Обновление ESET Cyber Security Pro до новой версии

Для обеспечения максимальной защиты важно использовать новейшую сборку ESET Cyber Security Pro. Чтобы проверить наличие новой версии, щелкните элемент **Домашняя страница** в главном меню. Если доступна новая сборка, отобразится сообщение. Нажмите **Подробнее...**, чтобы вывести на экран новое окно с информацией о номере версии доступной сборки и перечнем изменений.

Нажмите кнопку **Да**, чтобы загрузить последнюю сборку, или нажмите кнопку **Не сейчас**, чтобы закрыть окно и загрузить обновление позже.

Если нажать кнопку **Да**, файл будет загружен в папку загрузок (или в папку по умолчанию, установленную в браузере). Когда файл будет загружен, запустите его и следуйте указаниям по установке. Ваши имя пользователя и пароль будут автоматически перенесены в новую установленную версию. Рекомендуется регулярно проверять наличие обновлений, особенно при выполнении установки ESET Cyber Security Pro с компакт- или DVD-диска.

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. Вы будете получать уведомления программы ESET Cyber Security Pro об отсутствующих обновлениях в соответствии с указанным уровнем безопасности. Доступность уведомлений об обновлениях можно регулировать в разделе **Настройка** > **Настроить параметры приложения ...** (или нажмите *cmd+,*) > **Предупреждения и уведомления > Настройка...** путем изменения **условий отображения** рядом с **обновлениями 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 пропущенных обновлениях, снимите флажок рядом с параметром **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. Выполнить обновление можно непосредственно в окне оповещения или в разделе **Домашняя страница** программы ESET Cyber Security Pro, щелкнув параметр **Установить пропущенное обновление**.

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.

Служебные программы

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

Файлы журнала

Файлы журнала содержат информацию о важных программных событиях и предоставляют сводные сведения об обнаруженных угрозах. Ведение журнала является важнейшим элементом анализа, обнаружения угроз и устранения проблем. Оно выполняется в фоновом режиме без вмешательства пользователя. Данные сохраняются в соответствии с текущими параметрами степени детализации журнала. Просматривать текстовые сообщения и файлы журнала, а также архивировать их можно непосредственно в среде ESET Cyber Security Pro.

Получить доступ к файлам журнала можно из главного меню ESET Cyber Security Pro, выбрав в нем **Служебные программы** > **Журналы**. Выберите нужный тип журнала в раскрывающемся меню **Журнал** в верхней части окна. Доступны следующие журналы:

1. **Обнаруженные угрозы**: используется для просмотра всех данных о событиях, связанных с обнаружением заражений.
2. **События**: этот журнал упрощает устранение проблем для системных администраторов и пользователей. В нем регистрируются все важные действия, выполняемые программой ESET Cyber Security Pro.
3. **Сканирование компьютера**: в этом журнале отображаются результаты всех выполненных сканирований. Чтобы получить подробную информацию о той или иной операции сканирования компьютера по требованию, дважды щелкните соответствующую запись.
4. **Родительский контроль**: список всех веб-страниц, заблокированных функцией родительского контроля.
5. **Файервол**: в этом журнале отображаются результаты всех событий, имеющих отношение к сети.
6. **Отфильтрованные веб-сайты**: этот список будет полезен при просмотре списка веб-сайтов, заблокированных функцией защиты доступа в Интернет. В этих журналах записывается время, URL-адрес, состояние, IP-адрес, сведения о пользователе и приложении, инициировавшем подключение к определенному веб-сайту.

Для того чтобы скопировать в буфер обмена информацию из любого раздела журнала, выделите необходимую запись и нажмите кнопку **Копировать**.

Обслуживание журнала

Конфигурация журнала ESET Cyber Security Pro доступна в главном окне программы. Последовательно выберите элементы **Настройка** > **Дополнительные настройки** (или

нажмите *cmd+,*) > **Файлы журналов**. Для файлов журнала можно задать параметры, указанные ниже.

- **Автоматически удалять устаревшие записи журнала**: данный параметр обеспечивает автоматическое удаление записей, которые хранятся в журнале дольше указанного количества дней (90 дней по умолчанию).
- **Автоматически оптимизировать файлы журналов**: включает автоматическую дефрагментацию файлов журналов при достижении указанной процентной доли неиспользуемых записей (25 % по умолчанию).

Всю соответствующую информацию, отображаемую в графическом интерфейсе и сообщениях об угрозах и событиях, можно сохранять в понятных для человека текстовых форматах, например в формате обычного текста или CSV (Comma-separated values). Если необходимо сделать эти файлы доступными для обработки в сторонних приложениях, установите флажок **Включить ведение журнала в текстовых файлах**.

Чтобы указать целевую папку для сохранения файлов журнала, нажмите кнопку **Настройка** рядом с элементом **Расширенные параметры**.

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.
- Все события, связанные с обменом данными через файервол, записываются в файл firewalllog.txt

Чтобы настроить **фильтры по умолчанию для записей журналов сканирования компьютера**, нажмите кнопку **Изменить** и выберите нужные типы журналов (или отмените их выбор). Дополнительные сведения об этих типах журналов приведены в разделе Фильтрация журнала.

Фильтрация журнала

В журналах хранится информация о важных системных событиях. Функция фильтрации журнала позволяет отобразить записи о событиях определенного типа.

Ниже указаны типы журналов, используемые чаще всего.

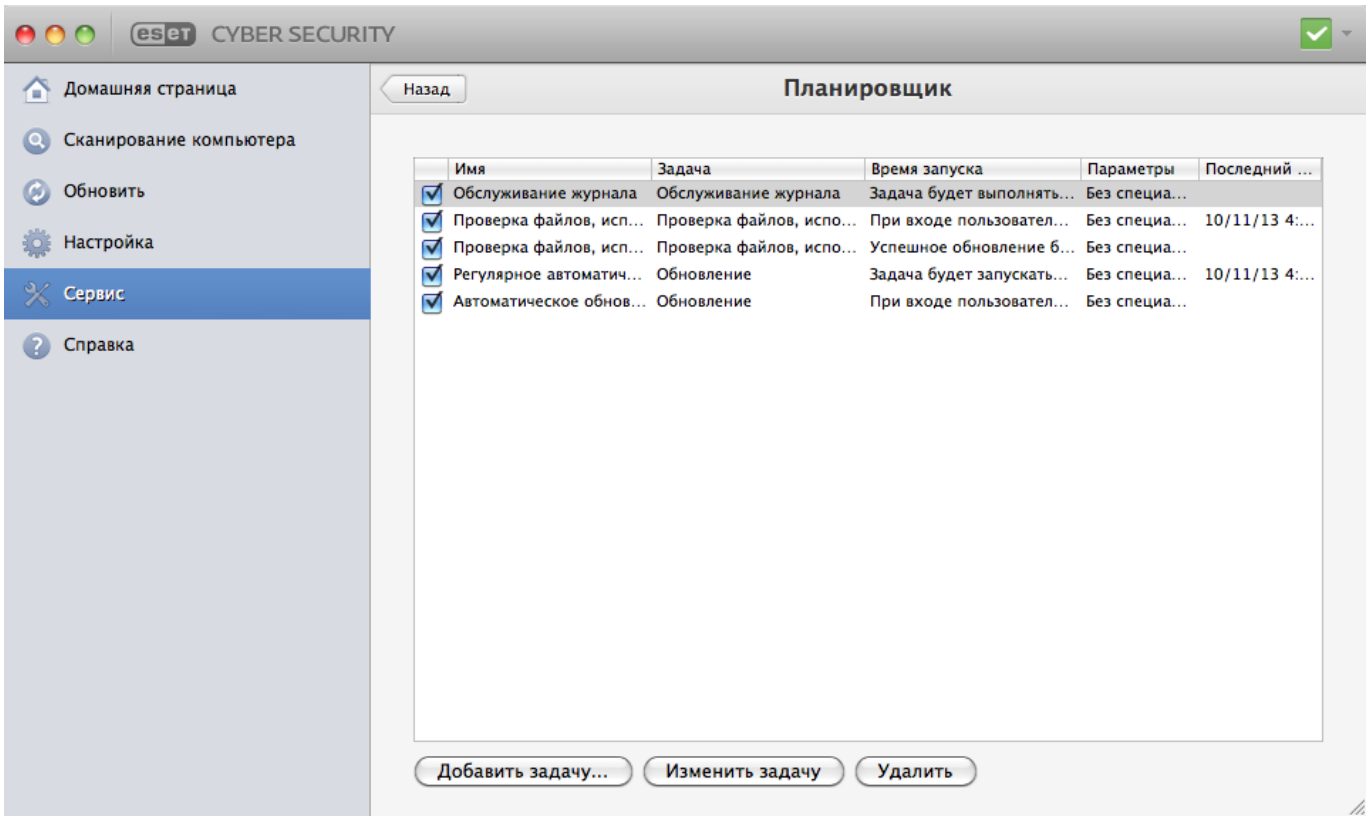
- **Критические предупреждения**: в эти журналы записываются критические системные ошибки (например, сбой запуска защиты от вирусов).
- **Ошибки**: в эти журналы записываются сообщения об ошибках типа «Не удалось загрузить файл» и критические ошибки.
- **Предупреждения**: в эти журналы записываются сообщения 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 Cyber Security Pro, воспользовавшись пунктом **Сервис**. **Планировщик** содержит полный список всех запланированных задач и их параметры запуска (дату, время и используемый профиль сканирования).



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

По умолчанию в планировщике отображаются следующие запланированные задачи:

• Обслуживание журнала (после установки флажка **Показывать системные задачи** при настройке 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 в планировщике задачу, нажмите кнопку **Добавить задачу** или щелкните пустое поле, удерживая клавишу CTRL, и выберите в контекстном меню команду **Добавить**. Доступно пять типов задач:

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

Запуск приложения

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

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**, 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. В конце появится окно со сводной информацией о текущей запланированной задаче. Нажмите кнопку **Готово**. Новая задача появится в списке запланированных.

В программе ESET Cyber Security Pro предусмотрены уже готовые запланированные задачи, которые обеспечивают правильную работу приложения. Изменять эти задачи нельзя, и по умолчанию они скрыты. Для того чтобы сделать эти задачи видимыми, в главном меню выберите пункт **Настройка** > **Дополнительные настройки** (или нажмите *cmd+,*) > **Планировщик** и установите флажок **Показывать системные задачи**.

Сканирование от имени владельца каталога

Каталоги можно сканировать от имени владельца каталога:

```
root:for VOLUME in /Volumes/*; do sudo -u \#`stat -
f %u "$VOLUME"` '/Applications/ESET Cyber Security.app/Contents/MacOS/esets_scan' -
f /tmp/scan_log "$VOLUME"; done
```

Кроме того, папку `/tmp` можно сканировать от имени вошедшего в систему пользователя:

```
root:sudo -u \#`stat -
f %u /dev/console` '/Applications/ESET Cyber Security.app/Contents/MacOS/esets_scan'
 /tmp
```

Создание пользовательских задач

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
```

Специальные символы, которые поддерживаются в выражениях cron, указаны ниже.

- звездочка (*): выражение соответствует всем значениям поля (например, звездочка в третьем поле — число месяца — означает любое число);
- дефис (-): задает диапазон, например3-9;
- 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.



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

Карантин

Карантин предназначен в первую очередь для безопасного хранения зараженных файлов. Файлы следует помещать на карантин, если они не могут быть очищены или безопасно удалены, если удалять их не рекомендуется или если они ошибочно отнесены программой ESET Cyber Security Pro к зараженным.

Поместить на карантин можно любой файл. Рекомендуется помещать на карантин файлы с подозрительной активностью, которые, тем не менее, не определяются модулем сканирования как зараженные. Файлы на карантине можно предоставить в лабораторию ESET для дальнейшего анализа.

Информацию о файлах, помещенных на карантин, можно просмотреть в виде таблицы, содержащей дату и время помещения зараженного файла на карантин, путь к его исходному расположению, его размер в байтах, причину помещения файла на карантин (например, мнение пользователя) и количество обнаруженных угроз (например, если архив содержит несколько заражений). Папка карантина с помещенными на карантин файлами () остается в системе даже после удаления программы ESET Cyber Security Pro. Файлы на карантине хранятся в безопасном зашифрованном виде. Их можно восстановить после повторной установки приложения ESET Cyber Security Pro.

Помещение файлов на карантин

Приложение ESET Cyber Security Pro автоматически помещает удаленные файлы на карантин (если вы не сняли флажок для этой функции в окне предупреждения). Вы можете отправить любой файл на карантин вручную, щелкнув вариант **Карантин...**. . Для этого также можно использовать контекстное меню. Удерживая клавишу CTRL, щелкните мышью в пустом поле, выберите **Карантин**, выделите файл, который нужно поместить на карантин, и нажмите кнопку **Открыть**.

Восстановление из карантина

Помещенные на карантин файлы также можно восстановить в их первоначальном расположении. Для этого нужно выбрать файл в папке карантина и щелкнуть **Восстановить**. Для восстановления также можно воспользоваться контекстным меню: удерживая клавишу CTRL, выберите нужный файл в окне карантина, а затем щелкните **Восстановить**. Контекстное меню содержит также функцию **Восстановить в...**, которая позволяет восстановить файл в месте, отличном от исходного.

Отправка файла из карантина

Если на карантин помещен файл, угроза в котором не распознана программой, или файл неверно квалифицирован как зараженный (например, в результате ошибки эвристического метода) и изолирован, передайте файл в лабораторию ESET. Чтобы отправить файл из карантина, щелкните его, удерживая клавишу CTRL, и в контекстном меню выберите пункт **Отправить файл на анализ**.

Запущенные процессы

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

• **Процесс**: имя процесса, запущенного в настоящий момент на компьютере. Для просмотра всех запущенных процессов можно также использовать монитор активности (находится в папке */Applications/Utilities*).

• **Уровень риска**: в большинстве случаев программа ESET Cyber Security Pro и технология ESET Live Grid присваивают уровни риска объектам (файлам, процессам и т. п.) с помощью ряда эвристических правил, которые проверяют характеристики каждого объекта, а затем оценивают их потенциальную способность к вредоносным действиям. На основании этого эвристического анализа объектам присваивается уровень риска. Известные приложения, помеченные зеленым цветом, являются определенно чистыми (находятся в белом списке) и исключаются из сканирования. Это повышает скорость как сканирования по требованию, так 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, можете отправить подозрительный файл в лабораторию ESET для анализа. Если окажется, что файл является вредоносным, его сигнатура будет добавлена в одно из ближайших обновлений.

• **Количество пользователей**: количество пользователей, использующих определенное приложение. Эта информация собирается технологией ESET Live Grid.

• **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.

Сетевые подключения

Сетевые подключения — это список активных сетевых подключений вашего компьютера. ESET Cyber Security Pro предоставляет подробную информацию о каждом подключении и позволяет создать правило для блокирования таких подключений.

Создание правила блокирования для этого подключения

ESET Cyber Security Pro позволяет создать правило блокирования для каждого подключения в диспетчере **Сетевые подключения**. Чтобы создать правило блокирования, щелкните нужное подключение правой кнопкой мыши и выберите пункт **Создать правило блокирования для этого подключения**.

1. Выберите **профиль** подключения, для которого необходимо создать правило, и введите имя правила. Выберите приложение, в отношении которого следует применить правило, или установите флажок, чтобы применить правило ко всем приложениям.
2. Выберите действие для подключения: отклонить (заблокировать) или разрешить подключение. Выберите направление соединения, в отношении которого должно применяться правило. Вы можете создать файл журнала для правила, щелкнув **Правило журнала**.
3. Выберите типы протоколов и портов для подключения. Выберите порт для службы или укажите диапазон портов в следующем формате: от–до.
4. Выберите целевой объект и заполните обязательное поле в зависимости от целевого объекта.

Live Grid

Система своевременного обнаружения Live Grid позволяет компании ESET постоянно и без промедления получать информацию о новых заражениях. Двунаправленная система своевременного обнаружения Live Grid создана с единственной целью — улучшить предлагаемую пользователям защиту. Лучший способ получения информации о новых угрозах незамедлительно после их появления — это поддержание связи с максимально возможным количеством пользователей и получение от них оперативных данных об угрозах. Существует два варианта работы.

1. Систему своевременного обнаружения Live Grid можно не включать. Программное обеспечение сохранит полную функциональность, и мы по-прежнему будем обеспечивать

для вас наилучшую защиту.

2. Систему своевременного обнаружения Live Grid можно настроить для отправки анонимной информации о новых угрозах и объектах, содержащих вредоносный код. Эта информация отправляется в компанию ESET для подробного анализа. Изучение этих угроз поможет компании ESET обновлять свой модуль обнаружения и улучшать возможности программы по обнаружению угроз.

Система своевременного обнаружения Live Grid 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 настройку Live Grid, в главном меню выберите пункт **Настройка** > **Настроить параметры приложения...** (или нажмите *cmd+,*) > **Live Grid**. Установите флажок **Включить систему своевременного обнаружения Live Grid**, чтобы активировать систему Live Grid, а затем нажмите кнопку **Настройка...** рядом с пунктом **Расширенные параметры**.

Настройка Live Grid

По умолчанию программа ESET Cyber Security Pro отправляет подозрительные файлы в лабораторию ESET для тщательного анализа. Если автоматическая отправка таких файлов не требуется, снимите флажок **Отправлять файлы**.

При обнаружении подозрительного файла его можно отправить в нашу лабораторию для анализа. Для этого в главном окне программы выберите **Служебные программы** > **Отправка образца на анализ**. Если файл окажется вредоносным приложением, следующее обновление будет его распознавать.

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

Фильтр исключений: этот параметр позволяет не отправлять определенные типы файлов. Например, это можно сделать для файлов, содержащих конфиденциальную информацию (документы или электронные таблицы). Файлы наиболее распространенных типов (.doc, .rtf и т. д.) по умолчанию не отправляются. В список исключаемых файлов можно добавить другие типы файлов.

Контактный адрес электронной почты (необязательно): ваш адрес электронной почты будет использован, если для анализа потребуются дополнительные данные. Обратите

внимание: компания ESET ответит только в том случае, если потребуется дополнительная информация.

Отправка образца на анализ

При обнаружении подозрительного файла на компьютере его можно отправить на анализ в исследовательскую лабораторию ESET.



Перед отправкой образцов в ESET

Вы можете отправлять только образцы, которые соответствуют по крайней мере одному из следующих критериев:
• Программа ESET не обнаруживает образец.
• Образец ошибочно обнаруживается как угроза.
• Мы не принимаем личные файлы (которые вы хотите просканировать на наличие вредоносных программ с помощью ESET) в качестве образцов (вирусная лаборатория ESET не проводит сканирование по запросу пользователей).
• Тема письма должна описывать проблему, а текст должен содержать как можно более полную информацию о файле (например, снимок экрана или адрес веб-сайта, с которого он был загружен).

Чтобы отправить образец, воспользуйтесь формой отправки образца в своем продукте. Чтобы открыть ее, нажмите **Инструменты** > **Отправка образца на анализ**.

В форме **Отправка образца на анализ** заполните следующие поля.

Файл: путь к отправляемому файлу.

Комментарий: описание причины, по которой вы отправляете файл.

Адрес электронной почты: адрес отправляется в ESET вместе с подозрительными файлами и может использоваться для запроса дополнительной информации, необходимой для анализа. Указывать адрес электронной почты необязательно.



Вы можете не получить ответа от ESET

Поскольку каждый день на серверы ESET поступают десятки тысяч файлов, невозможно отправить ответ на каждый запрос. Вам ответят только в том случае, если для анализа потребуется дополнительная информация.
Если образец окажется вредоносным приложением или веб-сайтом, его обнаружение будет добавлено при следующем обновлении программы ESET.

Интерфейс

Параметры конфигурации интерфейса позволяют настроить рабочую среду в соответствии с требованиями пользователя. Эти параметры доступны в главном меню в разделе **Настройка** > **Настроить параметры приложения...** (или нажмите *cmd+,*) > **Интерфейс**.

• Для отображения заставки ESET Cyber Security Pro при запуске системы установите флажок **Показывать заставку при запуске**.

• С помощью параметра **Поместить приложение на панель Dock** можно разместить значок ESET Cyber Security Pro на панели Dock в macOS, а также переключаться между программой ESET Cyber Security Pro и другими запущенными приложениями с помощью сочетания клавиш *cmd+TAB*. Изменения вступают в силу после повторного запуска программы ESET Cyber Security Pro (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).

• Чтобы включить подсказки для некоторых функций программы ESET Cyber Security Pro, установите флажок **Показывать подсказки**.

• Параметр **Показывать скрытые файлы** позволяет просматривать и выбирать скрытые файлы при настройке **объектов сканирования** в рамках **сканирования компьютера**.

• По умолчанию значок ESET Cyber Security Pro 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 Cyber Security Pro (обычно после перезагрузки компьютера).

Предупреждения и уведомления

Раздел **Предупреждения и уведомления** поможет настроить обработку предупреждений об угрозах и системных уведомлений в ESET Cyber Security Pro.

Если снять флажок **Отображать предупреждения**, предупреждения будут отключены, поэтому делать это без особых причин не рекомендуется. В большинстве случаев лучше оставить этот параметр без изменений (включенным). Описание расширенных параметров приводится 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 Cyber Security Pro 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 Cyber Security Pro 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**.

Список диалоговых окон (**Настройка** > **Ввести настройки приложения...** > **Предупреждения и уведомления** > **Настройка...**): отображается список всех диалоговых окон, которые отображаются при работе программы ESET Cyber Security Pro. Чтобы включить или отключить то или иное уведомление, установите флажок слева от **имени диалогового окна**. Кроме того, можно задать **условия отображения**, согласно которым будут отображаться уведомления о новых версиях программы и обновлении операционной системы.

Состояния защиты

Текущее состояние защиты программы ESET Cyber Security Pro 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 Cyber Security Pro (окно **Состояние защиты**).

Можно скрыть состояние защиты следующих компонентов программы:

- файервол;
- защита от фишинга;
- защита доступа в Интернет;
- защита почтового клиента;
- обновление операционной системы;
- окончание срока действия лицензии;
- требуется перезапуск компьютера.

Разрешения

Настройки ESET Cyber Security Pro могут иметь большое значение для политики безопасности вашей организации. Несанкционированное изменение параметров может нарушить стабильность работы системы и ослабить ее защиту. По этой причине вы можете сами определять пользователей, которым разрешается изменять конфигурацию программы.

Чтобы указать привилегированных пользователей, выберите **Настройка** > **Дополнительные настройки** (или нажмите *cmd+,*) > **Разрешения**. Выберите пользователей или группы из списка слева и щелкните **Добавить**. Чтобы отобразить всех пользователей и все группы системы, установите флажок **Показывать всех пользователей/все группы**. Чтобы удалить пользователя, выберите его имя в списке **Выбранные пользователи** в правой части окна и нажмите кнопку **Удалить**.



Об обновлении

Если список «Выбранные пользователи» пуст, все пользователи считаются привилегированными.

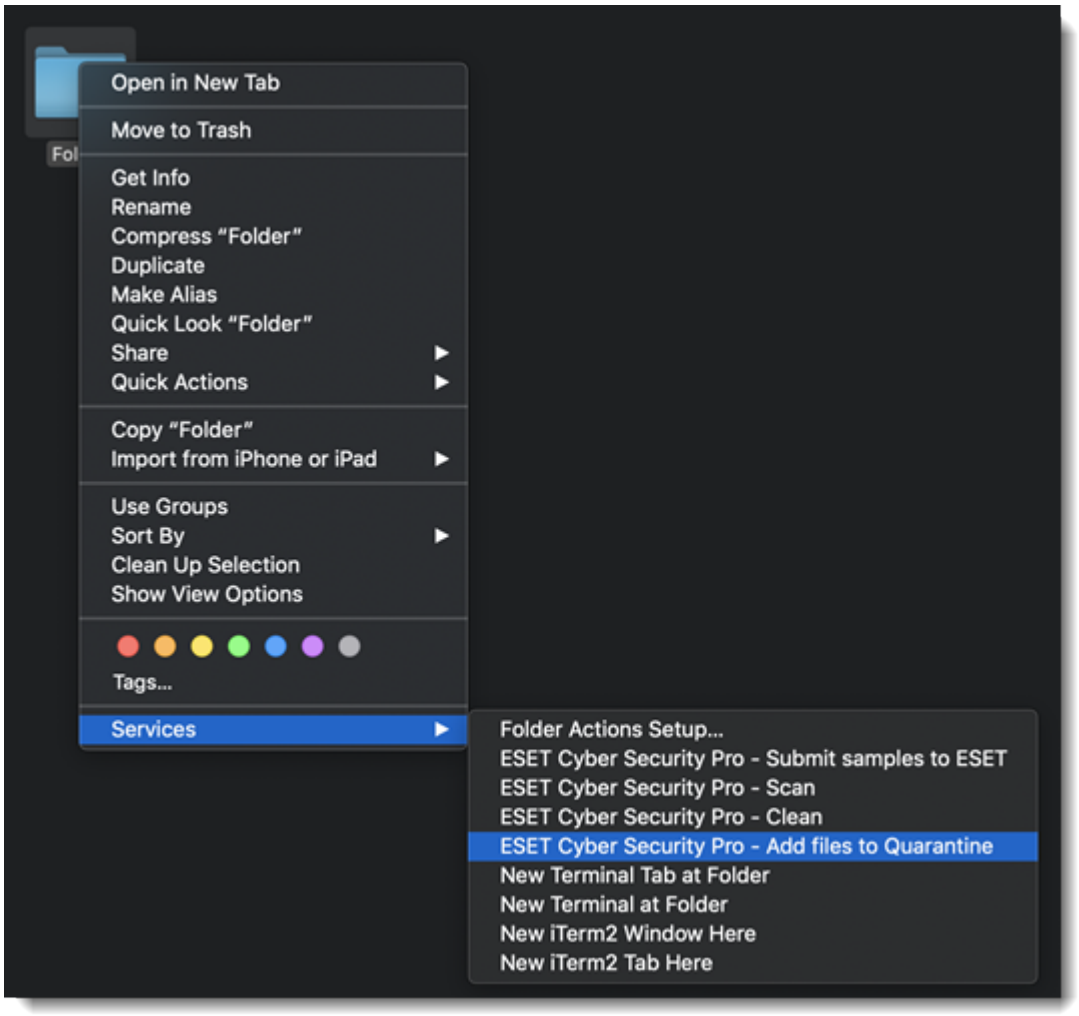
Контекстное меню

Чтобы включить интеграцию с контекстным меню, щелкните **Настройка** > **Дополнительные настройки** (или нажмите *cmd+,*) > **Контекстное меню**, установив флажок **Интеграция в контекстное меню**. Чтобы изменения вступили в силу, необходимо выйти из системы или перезагрузить компьютер. Пункты контекстного меню появятся в окне **Finder**, если щелкнуть любой файл, удерживая клавишу CTRL.

Вы можете выбрать параметры, которые будут отображаться в контекстном меню. Можно отобразить параметр **Только сканирование**, позволяющий сканировать выбранный файл, а параметр **Только очистка** позволяет запустить очистку выбранного файла из контекстного меню. 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, он будет удален.

Если выбрать параметр **Все**, с помощью контекстного меню можно выполнять следующие задачи:

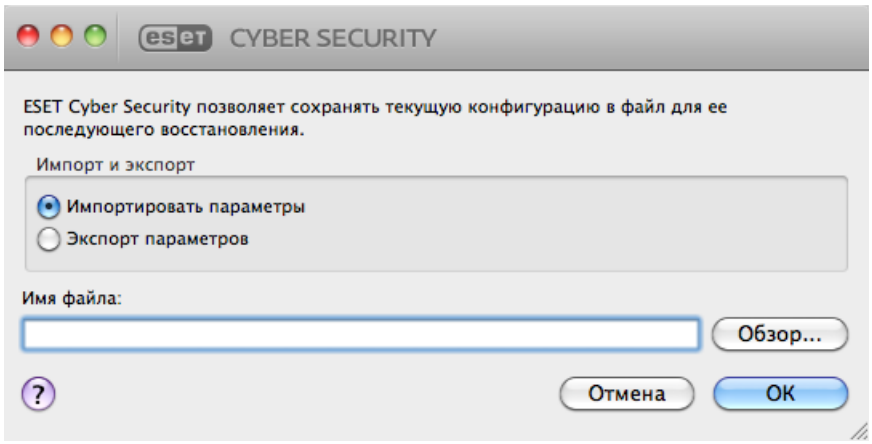
- Отправить образцы в ESET
- Сканирование
- Чистый
- Добавление файлов в карантин



Импорт и экспорт параметров

Чтобы импортировать существующую конфигурацию или экспортировать конфигурацию ESET Cyber Security Pro, последовательно выберите **Настройка** > **Импорт или экспорт параметров**.

Импорт и экспорт удобны, если нужно создать резервную копию текущей конфигурации ESET Cyber Security Pro для дальнейшего использования. Экспорт параметров также удобен для пользователей, которые хотят использовать желаемую конфигурацию ESET Cyber Security Pro в разных системах. Можно с легкостью импортировать файл конфигурации, чтобы передать необходимые настройки.



Для импорта конфигурации выберите **Импортировать параметры** и нажмите кнопку **Обзор**, чтобы перейти к файлу конфигурации, который необходимо импортировать. Для экспорта выберите элемент **Экспортировать параметры** и с помощью браузера выберите папку на компьютере, в которую необходимо сохранить файл конфигурации.

Настройка прокси-сервера

Для настройки параметров прокси-сервера выберите **Настройка** > **Ввести настройки приложения...** (или нажмите *cmd+,*) > **Прокси-сервер**. Настройка прокси-сервера на этом уровне позволяет задать его параметры для всех функций программы ESET Cyber Security Pro. Они используются всеми модулями программы, которым требуется подключение к Интернету. ESET Cyber Security Pro поддерживает следующие типы аутентификации: с базовым доступом 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 (по умолчанию 3128). Кроме того, можно щелкнуть **Обнаружить**, чтобы программа заполнила оба поля.

Если для обмена данными с прокси-сервером требуется аутентификация, введите правильные данные в поля **Имя пользователя** и **Пароль**.

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-a 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: HOM-ECS-20-01

Политика конфиденциальности

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