CYBER SECURITY PRO

для macOS

Руководство пользователя

(для версии продукта 6.0 и выше)

Щелкните здесь, чтобы загрузить последнюю версию этого документа.

Служба поддержки клиентов: www.eset.com/support

REV. 19. 9. 2016

Содержание

1. 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.

1.1 Новые возможности версии 6

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

- **Защита от фишинга**. Данная функция предотвращает предоставление ваших личных данных фиктивным веб-сайтам, которые имитируют надежность.
- **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 17.
- **Состояния защиты**. Этот параметр скрывает уведомления с экрана состояния защиты (например, *Защит а элект ронной почт ы от ключена* или *Требует ся перезагрузка компьют ера*).
- **Носители для сканирования**. Определенные типы носителей можно исключать из сканирования в режиме реального времени (локальные диски, съемные носители, сетевые носители).

1.2 Системные требования

Для оптимальной работы ESET Cyber Security Pro система должна отвечать указанным ниже требованиям к оборудованию и программному обеспечению или превышать их.

	Системные требования
Архитектура процессора	Intel, 32- или 64-разрядная
Операционная система	macOS 10.6 или более поздней версии
Память	300 МБ
Свободное место	200 МБ

2. Установка

Прежде чем приступать к процессу установки, нужно закрыть все открытые 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 компакт- или DVD-диска, вставьте его в дисковод, откройте на рабочем столе или в окне **Finder** и дважды щелкните значок **Установить**.
- Если установка выполняется с помощью файла, загруженного с веб-сайта ESET, откройте его и дважды щелкните значок **Установить**.

Мастер установки поможет вам настроить основные параметры приложения. На начальной стадии установки установщик автоматически проверит в Интернете наличие последней версии программы. При наличии более новой версии система предложит вам загрузить ее, прежде чем продолжить процесс установки.

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

- Обычная установка 4
- Выборочная установка 5

2.1 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.

ESET Live Grid
Система своевременного обнаружения Live Grid помогает компании ESET незамедлительно и постоянно получать информацию о новых заражениях, чтобы иметь возможность быстро защищать своих пользователей. Система обеспечивает отправку новых угроз в лабораторию ESET, где они анализируются, обрабатываются и добавляются в базу данных сигнатур вирусов. Параметр **Включить ESET Live Grid (рекомендуется)** по умолчанию включен. Нажмите кнопку

Настройка..., чтобы изменить детальные настройки отправки подозрительных файлов. Дополнительные сведения см. в разделе Live Grid 21.

Потенциально нежелательные приложения
Последним действием при установке является настройка обнаружения **потенциально нежелательных приложений**. Такие программы могут не быть вредоносными, однако они часто негативно влияют на работу операционной системы. Такие приложения часто поставляются в пакете с другими программами, и их установку бывает трудно заметить при установке всего пакета. Хотя при установке таких приложений обычно на экран выводится уведомление, они вполне могут быть установлены без согласия пользователя.

После установки ESET Cyber Security Pro следует выполнить сканирование компьютера на предмет наличия вредоносного кода. В главном окне программы выберите пункт **Сканирование компьютера**, а затем — **Сканирование Smart**. Дополнительные сведения о сканировании ПК по требованию см. в разделе Сканирование ПК по требованию 9.

2.2 Выборочная установка

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

Прокси-сервер
Если используется прокси-сервер, можно указать его параметры, установив флажок **Я использую прокси-сервер**. В следующем окне введите IP-адрес или URL-адрес прокси-сервера в поле **Адрес**. В поле «Порт» укажите порт, по которому прокси-сервер принимает запросы на соединение (по умолчанию 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 уверены насчет того, используется прокси-сервер или нет, можно использовать текущие системные параметры, установив флажок **Системные параметры (рекомендуется)**.

Разрешения
На следующем этапе можно определить особых пользователей или группы пользователей, которые смогут изменять конфигурацию 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 Live Grid
Система своевременного обнаружения Live Grid помогает компании ESET незамедлительно и постоянно получать информацию о новых заражениях, чтобы иметь возможность быстро защищать своих пользователей. Система обеспечивает отправку новых угроз в лабораторию ESET, где они анализируются, обрабатываются и добавляются в базу данных сигнатур вирусов. Параметр **Включить ESET Live Grid (рекомендуется)** по умолчанию включен. Нажмите кнопку **Настройка...**, чтобы изменить детальные настройки отправки подозрительных файлов. Дополнительные сведения см. в разделе Live Grid 21.

Потенциально нежелательные приложения
Следующим этапом установки является настройка обнаружения **потенциально нежелательных приложений**. Такие программы могут не быть вредоносными, однако они часто негативно влияют на работу операционной системы. Такие приложения часто поставляются в пакете с другими программами, и их установку бывает трудно заметить при установке всего пакета. Хотя при установке таких приложений обычно на экран выводится уведомление, они вполне могут быть установлены без согласия пользователя.

Файервол
В последнем шаге для файервола можно выбрать режим фильтрации. Дополнительные сведения см. в разделе Режимы фильтрации 13.

После установки ESET Cyber Security Pro следует выполнить сканирование компьютера на предмет наличия вредоносного кода. В главном окне программы выберите пункт **Сканирование компьютера**, а затем — **Сканирование Smart**. Дополнительные сведения о сканировании ПК по требованию см. в разделе Сканирование ПК по требованию 9.

3. Активация программы

После установки окно активации программы отобразится автоматически. Чтобы открыть диалоговое окно активации программы в любое время, щелкните значок ESET Cyber Security Pro, расположенный в строке меню macOS (верхняя часть 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 программы, 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 окно my.eset.com, где можно будет получить лицензионный ключ на основании имени пользователя и пароля.
- **Бесплатное БЕТА-тестирование**: выберите этот вариант, если перед приобретением вы желаете оценить программу ESET Cyber Security Pro. Укажите свой адрес электронной почты, чтобы активировать ESET Cyber Security Pro на ограниченный период времени. Ваша пробная 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 позднее**: выберите этот вариант, если активация в данный момент не требуется.

4. 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**.

5. 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 9.
- **Обновление**: выводит на экран информацию об обновлениях базы данных сигнатур вирусов.
- **Настройка**: этот раздел позволяет настроить уровень безопасности компьютера.
- **Сервис**: этот пункт предоставляет доступ к файлам журнала 18, планировщику 19, карантину 20, запущенным процессам 20 и другим возможностям программы.
- **Справка**: обеспечивает доступ к файлам справки, базе знаний в Интернете, форме запроса на получение поддержки и дополнительной информации о программе.

5.1 Сочетания клавиш

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

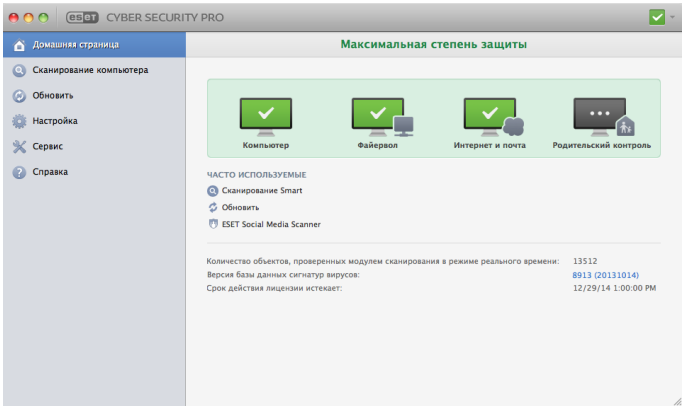
- *cmd+,*: отображает настройки ESET Cyber Security Pro.
- *cmd+O*: позволяет восстановить размер по умолчанию главного окна графического интерфейса программы ESET Cyber Security Pro и переместить его в центр экрана.
- *cmd+Q*: позволяет скрыть главное окно графического интерфейса программы ESET Cyber Security Pro. Его можно открыть, щелкнув значок ESET Cyber Security Pro ⓔ в строке меню macOS (вверху экрана).
- *cmd+W*: позволяет закрыть главное окно графического интерфейса программы ESET Cyber Security Pro.

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

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

5.2 Проверка состояния защиты

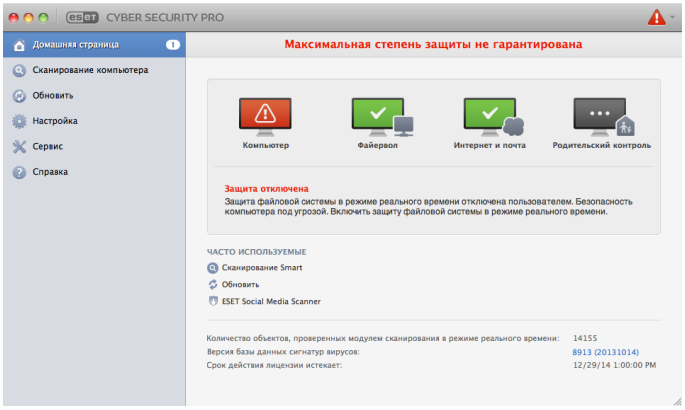
Чтобы просмотреть состояние защиты, в главном меню откройте вкладку **Домашняя страница**. В основном окне появится сводная информация о работе модулей ESET Cyber Security Pro.



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

Если модуль работает должным образом, отображается зеленый значок. Если модуль работает ненадлежащим образом, отображается 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 разрешить 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.



6. 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...**.

6.1 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.

6.1.1 Общие

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

- **Потенциально нежелательные приложения**: такие приложения не обязательно являются вредоносными, но могут тем или иным образом снижать производительность системы. Такие приложения обычно запрашивают при установке согласие пользователя. После их установки работа системы изменяется. Наиболее заметны такие изменения, как появление нежелательных всплывающих окон, запуск скрытых процессов, увеличение степени использования системных ресурсов, изменение результатов поисковых запросов и обмен данными с удаленными серверами.
- **Потенциально опасные приложения**: в эту категорию входит коммерческое законное программное обеспечение, которым могут воспользоваться злоумышленники, если такие приложения были 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 7, нажмите кнопку **Настройка...**.

6.1.1.1 Исключения

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

Файлы и папки, содержащиеся 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 исключается из сканирования не полностью, а только для указанной угрозы. Если файл окажется заражен другой вредоносной программой, модуль защиты от вирусов ее обнаружит.
- [+]: создание исключения. Укажите путь к объекту (допускается использование подстановочных знаков * (звездочка) и ? (знак вопроса)) либо выберите папку или файл в структуре дерева.
- [−]: удаление выделенных записей.
- **По умолчанию**: отмена всех исключений.

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

6.1.2 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 и после успешного обновления базы данных вирусов. Чтобы изменить параметры модуля ThreatSense, применимые к сканированию при запуске системы, нажмите кнопку **Настройка...**. Дополнительные сведения о настройке модуля ThreatSense приведены в этом разделе 10.

6.1.3 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 10) 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 указанные 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 прервать, 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 8).

6.1.3.1 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 10.

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 системы 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.

6.1.3.2 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**).

6.1.3.3 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.

6.1.3.4 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**.

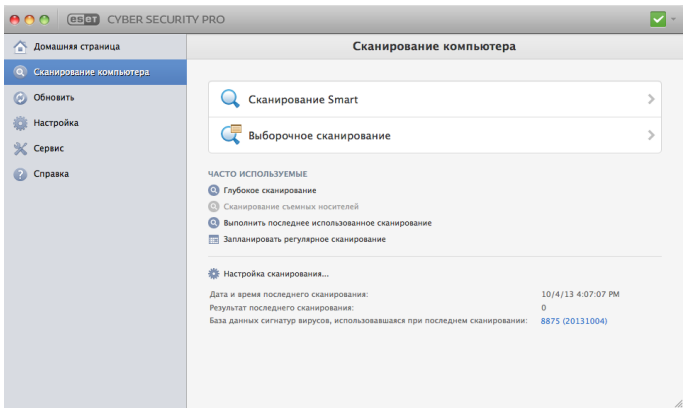
Функция защиты в режиме реального времени не обнаруживает и не очищает заражения
Убедитесь, что на компьютере не установлены другие программы защиты от вирусов. При одновременной работе двух систем защиты в режиме реального времени могут возникать конфликты. Рекомендуется удалить все другие программы 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 поддержки клиентов ESET.

6.1.4 Сканирование компьютера по требованию

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

Рекомендуется запускать сканирование ПК по требованию хотя бы раз в месяц. Можно сконфигурировать сканирование в качестве запланированной задачи в разделе **Служебные программы** > **Планировщик**.



Рекомендуется запускать сканирование ПК по требованию хотя бы раз в месяц. Можно сконфигурировать сканирование в качестве запланированной задачи в разделе **Служебные программы** > **Планировщик**.

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

6.1.4.1 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.

6.1.4.1.1 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 11.

6.1.4.1.2 Выборочное сканирование

Выборочное сканирование является оптимальным решением в том случае, если нужно указать параметры сканирования (например, объекты и методы сканирования). Преимуществом такого сканирования является возможность детальной настройки параметров. Различные конфигурации можно сохранить в виде пользовательских профилей сканирования — это удобно, если сканирование выполняется регулярно с использованием одинаковых параметров.

Чтобы указать объекты сканирования, выберите пункт **Сканирование компьютера** > **Выборочное сканирование** и отметьте нужные **объекты сканирования** в древовидной структуре. Объекты сканирования также можно задать более точно, указав пути к папкам и файлам, которые нужно сканировать. Если требуется только просканировать систему без выполнения дополнительных действий по ее очистке, выберите параметр **Сканировать без очистки**. Кроме того, можно выбрать один из трех уровней очистки в разделе **Настройка...** > **Очистка**.

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

6.1.4.2 Объекты сканирования

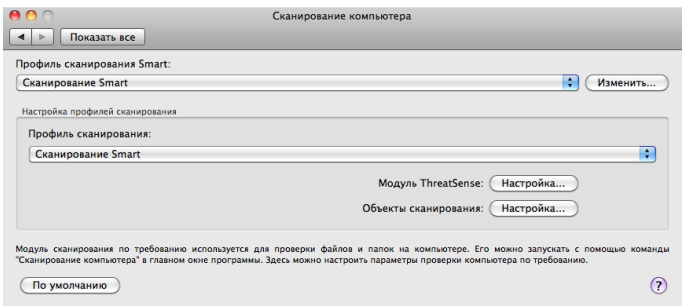
Древовидная структура объектов сканирования позволяет выбрать файлы и папки, которые необходимо просканировать на наличие вирусов. Выбор папок может также осуществляться в соответствии с параметрами профиля.

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.

6.1.4.3 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 10.

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 после сканирования работа операционной системы была завершена, а компьютер выключен, воспользуйтесь параметром **Выключение компьютера после сканирования**.

6.1.5 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, сигнатуры вирусов), 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 настройки, выберите **Настройка > Настроить параметры приложения...** (или нажмите *cmd+,*), а затем нажмите кнопку **Настройка...** модуля ThreatSense в разделах **Защита при запуске**, **Защита в режиме реального времени** и **Сканирование компьютера**, в которых используется технология 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.

6.1.5.1 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).
- **Упаковщики**: в отличие от стандартных архивов программы-упаковщики распаковывают файлы в системную память. При выборе этого параметра сканируются также стандартные статические упаковщики (например, UPX, yoda, ASPack, FGS).

6.1.5.2 Параметры

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

- **Эвристический анализ**: при эвристическом анализе используется алгоритм, который анализирует активность программ на предмет вредоносных действий. Основным преимуществом обнаружения путем эвристического анализа является возможность обнаруживать новые вредоносные программы, сведения о которых еще не попали в список известных вирусов (базу данных сигнатур вирусов).
- **Расширенная эвристика**: этот метод основан на уникальном эвристическом алгоритме компании ESET, оптимизированном для обнаружения компьютерных червей и троянских программ, написанных на языках программирования высокого уровня. Применение расширенной эвристики существенно улучшает возможности обнаружения вредоносных программ.

6.1.5.3 Очистка

Параметры очистки определяют способ очистки зараженных файлов модулем сканирования. Предусмотрено три уровня очистки, сведения о которых приведены ниже.

- **Без очистки**: зараженные файлы не очищаются автоматически. Программа выводит на экран предупреждение и предлагает пользователю выбрать нужное действие.
- **Стандартная очистка:** программа пытается автоматически очистить или удалить зараженный файл. Если невозможно автоматически выбрать правильное действие, пользователю предлагается сделать выбор. Выбор последующих действий предоставляется и в том случае, если предопределенное действие не может быть выполнено.
- **Тщательная очистка**: программа очищает или удаляет все зараженные файлы (в том числе архивы). Единственное исключение — системные файлы. Если очистить файл невозможно, вы получите оповещение с предложением выбрать тип действия, которое необходимо выполнить.

Предупреж дение. В стандартном режиме очистки, который используется по умолчанию, архив удаляется целиком только в том случае, если все файлы в нем заражены. Если в архиве помимо зараженных файлов имеются также незараженные файлы, такой архив удаляться не будет. Если зараженный файл в архиве обнаружен в режиме тщательной очистки, архив удаляется целиком, даже если в нем есть незараженные файлы.

6.1.5.4 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

6.1.5.5 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.

6.1.5.6 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 (ветвление ресурсов или 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.

6.1.6 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.).

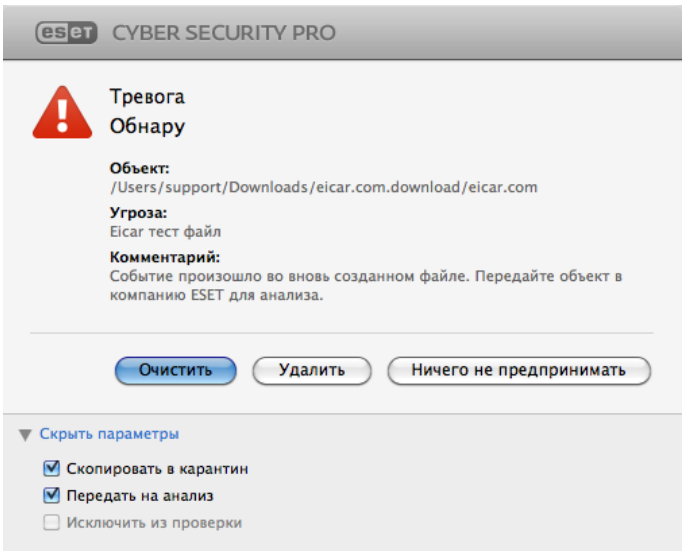
Если наблюдаются признаки заражения компьютера (например, он стал медленнее работать, часто «зависает» и т. п.), рекомендуется выполнить действия, описанные ниже.

1. Щелкните **Сканирование компьютера**.
2. Выберите параметр **Сканирование Smart** (дополнительную информацию см. в разделе Сканирование Smart 9).
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.

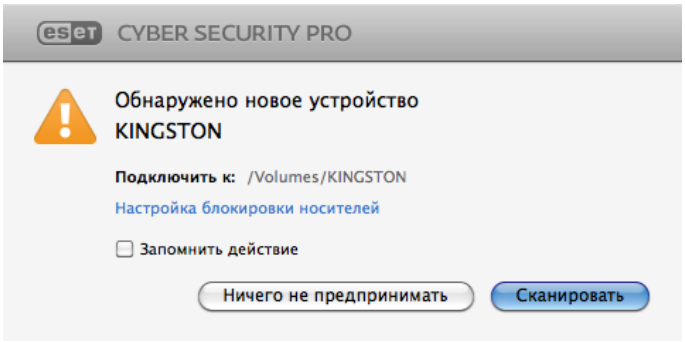
Очистка и удаление. Используйте очистку, если файл был атакован вирусом, добавившим в него вредоносный код. В этом случае в первую очередь следует попытаться очистить файл, чтобы восстановить его первоначальное состояние. Если файл содержит только вредоносный код, его следует удалить.



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.

6.2 Сканирование и блокирование съемных носителей

ESET Cyber Security Pro дает возможность выполнять сканирование по требованию для вставленных в компьютер съемных носителей (компакт- и DVD-дисков, USB-накопителей, устройств iOS и т. д.).



Съемные носители могут содержать вредоносный код и подвергать компьютер риску. Чтобы заблокировать съемный носитель, щелкните **Настройка блокировки носителей** (см. изображение выше) или в главном окне программы выберите в главном меню **Настройка** > **Настроить параметры приложения...** > **Носитель** и установите флажок **Включить блокирование съемных носителей**. Чтобы разрешить доступ к носителям определенного типа, снимите соответствующие флажки.

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

7. Защита от фишинга

Термином *фишинг* обозначается преступная деятельность с использованием методов 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.

Рекомендуем держать включенной функцию защиты от фишинга (**Настройка** > **Настроить параметры приложения...** > **Защита от фишинга**). Все потенциальные фишинговые атаки с веб-сайтов или доменов, занесенных компанией ESET в базу данных вредоносного ПО, блокируются, а для пользователя отображается уведомление об атаке.

8. Файервол

Персональный файервол контролирует весь входящий и исходящий сетевой трафик путем разрешения или запрещения отдельных сетевых подключений на основании заданных правил фильтрации. Он обеспечивает защиту от атак с удаленных компьютеров и позволяет блокировать некоторые службы. Он также обеспечивает защиту от вирусов для протоколов HTTP, POP3 и IMAP.

Конфигурацию персонального файервола можно найти, выбрав **Настройка** > **Файервол**. Она позволяет настроить режим, правила и детальные параметры фильтрации. Здесь можно также просмотреть более детальные настройки программы.

Если для параметра **Блокировать весь сетевой трафик: отключить сеть** установить значение **ВКЛЮЧЕНО**, весь входящий и исходящий трафик будет заблокирован персональным файерволом. Этот параметр следует использовать при подозрении наличия критических угроз безопасности, требующих отключения компьютера от сети.

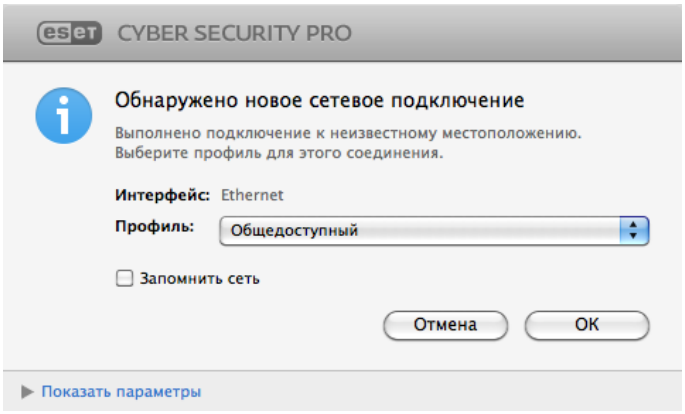
8.1 Режимы фильтрации

Для персонального файервола программы ESET Cyber Security Pro доступны три режима фильтрации. Параметры режимов фильтрации можно найти в настройках программы ESET Cyber Security Pro (нажмите *cmd+,*) > **Файервол**. Работа файервола изменяется в зависимости от выбранного режима. Режимы фильтрации также влияют на уровень необходимого взаимодействия с пользователем.

Весь трафик блокируется: весь входящий и исходящий трафик будет заблокирован.

Автоматически с исключениями: режим по умолчанию. Данный 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 все неинициированные соединения со стороны сети. Можно также добавить настраиваемые пользовательские правила.

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



Чтобы записать подробную информацию обо всех заблокированных подключениях в файл журнала, выберите параметр **Регистрировать все заблокированные соединения**. Для просмотра файлов журналов файервола в главном меню выберите пункт **Служебные программы** > **Журналы** и в раскрывающемся меню **Журнал** выберите пункт **Файервол**.

8.2 Правила для файервола

Правила представляют собой набор условий для проверки всех сетевых подключений и определяют действия, назначенные для этих условий. С помощью правил персонального файервола можно определить тип необходимого действия при установке обозначенного правилом подключения.

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

Обнаружив новое неизвестное вам подключение, хорошо подумайте, прежде чем разрешить или запретить 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 частных данных, а также загрузки других вредоносных приложений на рабочие станции узла. Персональный файервол позволяет обнаружить и разорвать такие подключения.

8.2.1 Создание новых правил

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

Чтобы создать правило, нажмите кнопку **Добавить...**, укажите имя правила и перетащите значок приложения в пустое поле или нажмите кнопку **Обзор...**, чтобы найти программу в папке */Applications*. Чтобы применить правило ко всем приложениям, установленным на компьютере, выберите параметр **Все приложения**.

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**.

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.

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

8.3 Зоны файервола

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

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

8.4 Профили файервола

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

8.5 Журналы файервола

Персональный файервол ESET Cyber Security Pro сохраняет все важные события в файл журнала. Для просмотра журналов файервола в главном меню выберите пункт **Сервис** > **Журналы** и в раскрывающемся меню **Журнал** выберите пункт **Файервол**.

Файлы журнала являются ценным средством для обнаружения ошибок и вторжений в систему. Журналы персонального файервола ESET содержат следующие сведения.

- Дата и время события
- Имя события
- Источник
- Целевой сетевой адрес
- Сетевой протокол связи
- Применяемое правило
- Используемое приложение
- Пользователь

Тщательный анализ этих данных поможет обнаружить попытки нарушить безопасность системы. Существует много других факторов, которые указывают на потенциальные угрозы безопасности и от которых можно избавиться с помощью персонального файервола, например: частые подключения из неизвестных местоположений, многочисленные попытки подключения, передача данных неизвестными приложениями или необычные номера портов.

9. Защита доступа в Интернет и электронной почты

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

- **Защита доступа в Интернет**: эта функция отслеживает обмен данными между веб-браузерами и удаленными серверами по протоколу HTTP.
- **Защита почтового клиента**: эта функция позволяет контролировать обмен сообщениями по протоколам POP3 и IMAP.
- **Защита от фишинга**: данная функция блокирует потенциальные фишинговые атаки с веб-сайтов и доменов, занесенных компанией ESET в базу данных вредоносных программ.

9.1 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 14 и/или URL-адреса 14.

9.1.1 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.

9.1.2 Списки URL-адресов

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

Чтобы разрешить доступ только к 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.

9.2 Защита электронной почты

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

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

Добавить уведомление к сноске сообщений электронной почты: после сканирования сообщения в него добавляется уведомление с результатами сканирования. На эти уведомления нельзя полагаться абсолютно, поскольку они могут быть пропущены в проблематичных сообщениях в формате HTML или фальсифицированы некоторыми вирусами. Доступны указанные ниже варианты.

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

Добавлять примечание в поле темы полученных и прочитанных зараженных сообщений: установите этот флажок, если требуется, чтобы модуль защиты электронной почты добавлял предупреждение о вирусе в зараженные письма. 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 добавления к теме зараженных писем: отредактируйте этот шаблон, если требуется изменить формат префикса темы для зараженных писем.

В нижней части этого окна можно включать и отключать проверку обмена сообщениями электронной почты по протоколам POP3 и IMAP. Подробные сведения об этом см. в следующих разделах:

- Проверка протокола POP3 15
- Проверка протокола IMAP 15

9.2.1 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.

9.2.2 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.

10. Родительский контроль

Используя раздел **Родительский контроль** можно настраивать параметры родительского контроля, который обеспечивает 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 оскорбительные материалы. Кроме того, родители имеют возможность запретить доступ к веб-сайтам 27 предварительно определенных категорий.

Учетные записи пользователей перечислены в окне **Родительский контроль** (**Настройка** > **Ввести настройки приложения...** > **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** выберите один из предопределенных профилей в раскрывающемся меню **Настройка профиля** 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 относятся к данной категории.

Чтобы изменить список **Разрешенные и заблокированные веб-страницы**, щелкните **Настройка...** в нижней части окна и добавьте имя домена в нужный список. Не следует 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.

ПРИМЕЧАНИЕ. Блокирование или разрешение отдельных веб-страниц может быть более точным, чем блокирование или разрешение целой категории веб-страниц.

11. Обновление

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

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 вручную запустить процесс обновления, щелкните **Обновить базу данных сигнатур вирусов**.

Обычно после корректного завершения загрузки в окне обновления выводится сообщение **Обновление не обязательно: установленная база данных сигнатур вирусов актуальна**. Если обновить базу данных сигнатур вирусов невозможно, рекомендуется проверить настройки обновления 16, так как самая распространенная причина этой ошибки — неверно введенные данные для аутентификации (имя пользователя и пароль) или некорректно выбранные параметры подключения 23.

В окне обновления также выводятся сведения о версии базы данных сигнатур вирусов. Этот числовой индикатор представляет собой активную ссылку на веб-сайт ESET со списком всех сигнатур, добавленных во время текущего обновления.

11.1 Настройка обновления

Для аутентификации на сервере обновлений ESET используются имя пользователя и пароль, созданные и отправленные вам после приобретения.

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

11.1.1 Расширенные параметры

Для отключения уведомлений, отображаемых после каждого успешно выполненного обновления, установите флажок **Не отображать уведомления о завершении обновления**.

Включите параметр **Тестовое обновление**, чтобы загружать разрабатываемые модули на этапе финального тестирования. Тестовые обновления зачастую содержат исправления программных ошибок. **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.

ESET Cyber Security Pro записывает моментальные снимки базы данных сигнатур вирусов и программных модулей для использования с функцией **Откат обновления**. Оставьте включенным параметр **Создавать снимки файлов обновлений**, чтобы программа ESET Cyber Security Pro записывала такие мгновенные снимки автоматически. Если вы подозреваете, что новое обновление базы данных вирусов и/или программных модулей работает неустойчиво или является поврежденным, можно выполнить откат к предыдущей версии и отключить обновления на заданный период времени. Кроме того, можно включить отключенные ранее обновления, если они были отложены на неопределенный период. При откате к предыдущему обновлению используйте раскрывающееся меню **Установить такой период приостановки**, чтобы указать период, на который следует отложить обновления. При выборе варианта **до отмены** обычные обновления можно будет возобновить только вручную. Выбирать этот параметр следует с осторожностью.

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

11.2 Создание задач обновления

Обновления можно запускать вручную. Для этого щелкните элемент **Обновление** в главном меню, а затем **Обновить базу данных сигнатур вирусов**.

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 19.

11.3 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.

11.4 Обновления системы

Функция обновления системы macOS является важным компонентом, предназначенным для защиты пользователей от вредоносных программ. В целях обеспечения максимальной безопасности рекомендуется устанавливать эти обновления сразу же после их появления. 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 системной 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. Подробнее об этом инструменте можно узнать в руководстве softwareupdate — для этого введите команду `man softwareupdate` в окне **«Терминал»**. Рекомендовано только для опытных пользователей.

12. Сервис

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

12.1 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**.

12.1.1 Обслуживание журнала

Конфигурация журнала ESET Cyber Security Pro доступна в главном окне программы. Нажмите **Настройка** > **Настроить параметры приложения...** (или нажмите *cmd+*) > **Файлы журнала**. 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).
- **Оптимизировать файлы журналов автоматически**: 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 запись 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 пользоват еля и пароль*, *Не удает ся обновит ь базу данных сигнат ур вирусов* 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 firewalllog.txt

Чтобы конфигурировать **фильтры по умолчанию для записей журналов сканирования компьютера**, нажмите кнопку **Изменить** и выберите (или отмените выбор) нужные типы журналов. Дополнительные сведения об этих типах журнала приведены в главе Фильтрация журнала 18.

12.1.2 Фильтрация журнала

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

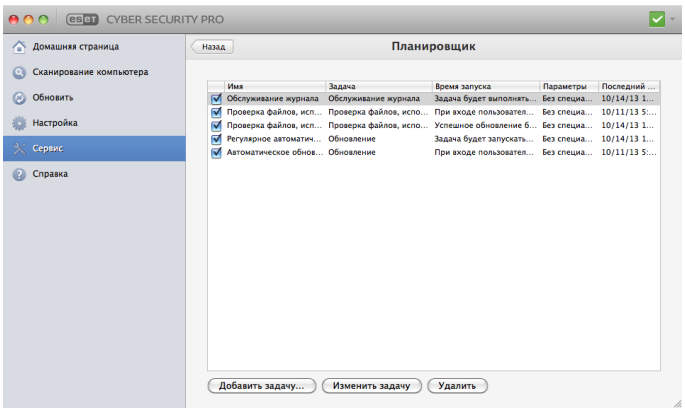
Ниже указаны типы журналов, используемые чаще всего.

- **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 загрузит ь 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.

12.2 Планировщик

Планировщик можно найти в главном меню ESET Cyber Security Pro, воспользовавшись пунктом **Служебные программы**. **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 после обновления базы данных сигнатур вирусов
- Регулярное автоматическое обновление
- Автоматическое обновление после входа пользователя в систему

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

12.2.1 Создание новых задач

Для того чтобы создать задачу в планировщике, нажмите кнопку **Добавить задачу...** или щелкните в пустом поле, удерживая клавишу CTRL, и выберите в контекстном меню команду **Добавить...**. Доступны пять типов запланированных задач. Они указаны ниже.

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

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

В приведенном ниже примере мы будем использовать планировщик для добавления новой задачи обновления, поскольку обновление является одной из наиболее часто используемых запланированных задач.

1. В раскрывающемся меню **Запланированная задача** выберите пункт **Обновление**.
2. Введите имя задачи в поле **Название задачи**.
3. Укажите частоту выполнения задачи в раскрывающемся меню **Выполнить задачу**. В зависимости от указанной частоты запуска будет предложено указать 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 19).
4. Затем укажите, какое действие следует предпринимать, если задача не может быть выполнена в установленное время.
5. В завершение появится окно со сводной информацией о текущей запланированной задаче. Нажмите кнопку **Завершить**. Новая задача будет добавлена в список текущих запланированных задач.

По умолчанию программа ESET Cyber Security Pro включает предопределенные запланированные задачи, которые обеспечивают правильную работу приложения. Изменить эти задачи нельзя, и по умолчанию они скрыты. Для того чтобы сделать эти задачи видимыми, в главном меню выберите пункт **Настройка** > **Настроить параметры приложения...** (или нажмите *cmd+,*) > **Планировщик** и установите флажок **Показывать системные задачи**.

12.2.2 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, например 3-9
- Запятая (,) — разделяет элементы списка, например 1,3,7,8
- Косая черта (/) — задает шаг диапазона, например 3-28/5 в третьем поле (число месяца) означает третье число любого месяца, а также другие числа с шагом пять дней

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

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

12.3 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 (*/Library/Application Support/Eset/esets/cache/quarantine*) 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.

12.3.1 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**.

12.3.2 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.

12.3.3 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**.

12.4 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 момента обнаружения приложения технологией ESET Live Grid.
- **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.

12.5 Live Grid

Система своевременного обнаружения Live Grid позволяет компании ESET незамедлительно и постоянно получать информацию о новых заражениях. Двунаправленная система своевременного обнаружения Live Grid создана с единственной целью — улучшить предлагаемую нами 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.

1. Можно не включать систему своевременного обнаружения Live Grid. Программное обеспечение сохранит полную функциональность, и мы по-прежнему будем обеспечивать для вас наилучшую защиту.
2. Можно конфигурировать систему своевременного обнаружения Live Grid для передачи анонимной информации о новых угрозах и объектах, содержащих новый код угроз. Эта информация может быть отправлена в компанию ESET для подробного анализа. Изучение этих угроз поможет компании ESET обновлять свою базу данных угроз и улучшать возможности программы по обнаружению угроз.

Система своевременного обнаружения Live Grid будет собирать о компьютере информацию, которая имеет отношение к новым обнаруженным угрозам. Эта информация может включать в себя образец или копию файла, в котором появилась угроза, путь к нему, имя файла, дату и время, процесс, благодаря которому угроза попала в компьютер, а также информацию об операционной системе компьютера.

Поскольку существует риск, что некоторая информация о вас или вашем компьютере (имена пользователя в пути к каталогу и т. п.) может случайно стать доступной для лаборатории ESET, 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** для активации Live Grid, а затем нажмите кнопку **Настройка...** рядом с пунктом **Расширенные параметры**.

12.5.1 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 это вредоносное приложение, его сигнатура будет включена в следующую версию базы данных сигнатур вирусов.

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.

Ниже приводится пример передаваемого пакета статистических данных:

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

Фильтр исключения: этот параметр позволяет исключить из отправки 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.

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.

13. Интерфейс пользователя

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 OS X, 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 6) и отображать элементы обычного меню («Интерфейс», «Настройка» и «Служебные программы») в строке меню OS X (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**.

13.1 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 22.

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 — 4 секунды).

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 22.

13.1.1 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.

13.1.2 Состояния защиты

Текущее состояние защиты программы ESET Cyber Security Pro можно изменить путем активации или деактивации состояний. Для этого нужно выбрать **Настройка** > **Настроить параметры 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
- Режим презентации
- Обновление операционной системы
- Окончание срока действия лицензии
- Необходимость перезагрузки компьютера

13.2 Разрешения

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

Чтобы указать пользователей с правами, выберите **Настройка** > **Настроить параметры приложения...** (или нажмите *cmd+,*) > **Разрешения**.

Для обеспечения максимальной безопасности компьютера принципиально важно правильно сконфигурировать программу. Несанкционированное изменение может привести к потере важных данных. Для составления списка пользователей с правами выберите их в списке **Пользователи** в левой части окна и нажмите кнопку **Добавить**. Чтобы отобразить всех пользователей, установите флажок **Показывать всех пользователей**. Чтобы удалить пользователя, выберите его имя в списке **Выбранные пользователи** в правой части окна и нажмите кнопку **Удалить**.

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

13.3 Контекстное меню

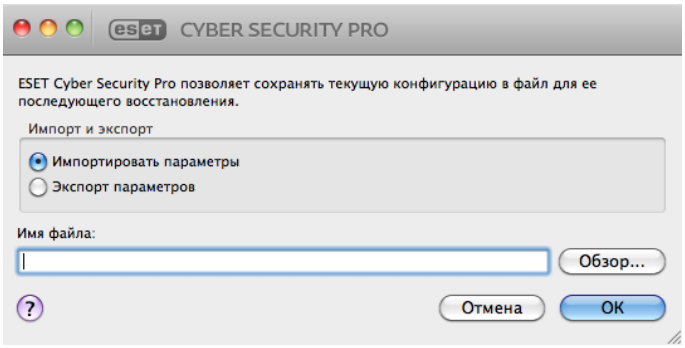
Для того чтобы включить интеграцию элементов в контекстное меню, щелкните **Настройка** > **Настроить параметры приложения...** (или нажмите *cmd+,*) > **Контекстное меню**, установив флажок **Интегрировать с контекстным меню**. Чтобы изменения вступили в силу, необходимо выйти из системы или перезагрузить компьютер. Пункты контекстного меню отображаются в окне **Finder**, если щелкнуть любой файл, удерживая клавишу CTRL.

14. Разное

14.1 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 **Импорт параметров** и нажмите кнопку **Обзор**, чтобы перейти к файлу конфигурации, который необходимо импортировать. Для экспорта выберите элемент **Экспорт параметров** и с помощью браузера выберите папку на компьютере, в которую необходимо сохранить файл конфигурации.

14.2 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 элемент **Обнаружить**, чтобы программа заполнила оба поля.

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

15. Глоссарий

15.1 Типы заражений

Заражение представляет собой попытки проникновения вредоносного программного обеспечения на компьютер пользователя и/или причинения ему вреда.

15.1.1 Вирусы

Компьютерный вирус — это такой вид заражения, который повреждает существующие файлы на компьютере. Название было выбрано из-за сходства с биологическими вирусами, так как они используют похожие методы для распространения с компьютера на компьютер.

Компьютерные вирусы обычно атакуют исполняемые файлы, сценарии и документы. Для размножения вирус присоединяет свое «тело» к концу заражаемого файла. Краткое описание цикла размножения: после запуска зараженного файла вирус активируется (перед активацией самого приложения) и выполняет свою задачу. Только после этого запускается само приложение. Вирус не может заразить компьютер, пока пользователь (по ошибке или намеренно) собственноручно не запустит файл с вредоносной программой.

Компьютерные вирусы могут быть разными по целям и степени опасности. Некоторые из вирусов особо опасны, так как могут удалять файлы с жесткого диска. В свою очередь другие вирусы не причиняют никакого вреда. Они просто досаждают пользователю, демонстрируя возможности своих авторов.

Важно отметить, что количество вирусов постоянно снижается по сравнению с троянскими и шпионскими программами, так как они не представляют для авторов экономической выгоды. Кроме того, термин «вирус» часто неправильно используют для описания всех возможных типов заражений. Однако постепенно он выходит из употребления, и на смену ему приходит более точный термин «вредоносная программа».

Если компьютер заражен вирусом, необходимо восстановить исходное состояние зараженных файлов. Обычно для этого выполняется очистка с помощью антивирусной программы.

15.1.2 Черви

Компьютерные черви — это содержащие злонамеренный код программы, которые атакуют главные компьютеры и распространяются через сеть. Основное различие между вирусами и червями заключается в том, что черви могут воспроизводиться и распространяться самостоятельно — они не зависят от зараженных файлов или загрузочных секторов. Черви распространяются, используя адресную книгу пользователя или уязвимости в системе безопасности сетевых приложений.

Черви намного более жизнеспособны, чем компьютерные вирусы. Благодаря Интернету они могут распространиться по всему земному шару за считанные часы после запуска в сеть. В некоторых случаях счет идет даже на минуты. Эта способность быстро самостоятельно реплицироваться делает черви более опасными, чем другие типы вредоносных программ.

Работающий в системе червь может доставить много неудобств пользователю: он может удалять файлы, снижать производительность системы или даже отключать другие программы. По сути компьютерный червь может служить в качестве «транспортного средства» для других типов заражений.

Если компьютер заражен червем, рекомендуется удалить инфицированные файлы, поскольку они содержат вредоносный код.

15.1.3 Троянские программы

Исторически троянскими программами называют особую группу вредоносных программ, которые выдают себя за полезные, чтобы пользователи запускали их. Сегодня троянские программы не нуждаются в подобной маскировке. Единственная их цель — как можно проще проникнуть в систему и запустить вредоносный код. Сегодня троянская программа — очень общий термин, используемый для обозначения любого заражения, которое невозможно отнести к какому-либо конкретному классу.

Так как эта категория весьма широка, ее часто разбивают на несколько подкатегорий.

- Программа-загрузчик — вредоносная программа, которая загружает другие вредоносные модули из Интернета.
- Программа-бомба — тип троянских программ, разработанных для заражения компьютеров другими вредоносными программами.
- Утилита удаленного администрирования — приложение, которое обменивается данными со злоумышленниками, позволяя им получить доступ к системе и контроль над ней.
- Клавиатурный шпион — такие программы записывают все, что пользователь набирает на клавиатуре, и отправляют эту информацию злоумышленникам.
- Программа дозвона — программы, которые пытаются набирать номера телефонов, звонки на которые оплачивает вызывающий абонент. При этом у пользователя практически нет шансов заметить, что создается новое подключение. Программы дозвона могут причинить вред только пользователям модемов. К счастью, модемы уже распространены не столь широко, как раньше.

Как правило, троянские программы распространяются в виде исполняемых файлов. Если на компьютере будет обнаружен файл, относящийся к категории троянских программ, рекомендуется удалить его, так как он скорее всего содержит вредоносный код.

15.1.4 Руткиты

Руткиты — это вредоносные программы, с помощью которых злоумышленники в Интернете получают неограниченный доступ к системе, скрывая следы своего присутствия. Получив доступ к системе (обычно с помощью уязвимости в ней), руткиты используют функции операционной системы, чтобы не дать антивирусному ПО себя обнаружить: они скрывают процессы и файлы. По этой причине их практически невозможно обнаружить с помощью обычных методов проверки.

15.1.5 Рекламные программы

Рекламными программами называют программное обеспечение, распространение которого обеспечивается за счет рекламы. Программы, демонстрирующие пользователю рекламу, попадают в эту категорию. Рекламные приложения часто автоматически открывают всплывающие окна с рекламой в веб-браузере или изменяют домашнюю страницу. Рекламные программы часто распространяются в комплекте с бесплатными. Это позволяет их создателям покрывать расходы на разработку полезных программ.

Сами по себе рекламные программы не опасны, но они доставляют неудобства пользователям. Опасность состоит в том, что в рекламных программах могут быть реализованы дополнительные функции слежения, как в шпионских программах.

Если принято решение использовать свободно распространяемый программный продукт, стоит уделить особое внимание программе установки. Чаще всего программа установки предупреждает об установке дополнительной рекламной программы. Часто пользователь имеет возможность отказаться от ее установки и установить только сам программный продукт без рекламной программы.

Некоторые программы нельзя установить без рекламных модулей, в противном случае их функциональность ограничивается. Это приводит к тому, что рекламная программа получает доступ к системе на «законных» основаниях, так как пользователь дал согласие на ее установку. В этом случает лучше заранее обезопасить себя, чем потом жалеть. В случае обнаружения файла, классифицированного как рекламная программа, рекомендуется удалить его, так как скорее всего он содержит вредоносный код.

15.1.6 Шпионские программы

К этой категории относятся все приложения, которые отправляют конфиденциальные данные злоумышленникам без ведома и согласия их владельца. Шпионские программы используют функции слежения для отправки различной статистической информации, такой как список посещенных веб-сайтов, адреса электронной почты из адресных книг пользователя или набираемый на клавиатуре текст.

Авторы шпионских программ утверждают, что эти методы служат для изучения требований и интересов пользователей и позволяют создавать рекламные материалы, более полно соответствующие интересам целевой аудитории. Проблема в том, что нет четкой границы между полезными и вредоносными приложениями, и никто не гарантирует, что собираемая информация не будет использована во вред. Данные, полученные шпионскими программами, могут содержать защитные коды, PIN-коды, номера счетов и т. д. Шпионские программы часто поставляются в комплекте с бесплатными версиями программ самими их авторами с целью получения доходов или стимулирования продаж программного обеспечения. Часто пользователей информируют о наличии шпионских программ во время установки основной программы, чтобы поощрить их к приобретению платной версии.

Примерами хорошо известного бесплатного программного обеспечения, вместе с которым поставляется шпионское ПО, могут служить клиенты пиринговых (P2P) сетей. Spyfalcon или Spy Sheriff (и многие другие) относятся к особой подкатегории шпионского ПО. Утверждается, что они предназначены для борьбы со шпионским ПО, но на самом деле они сами являются таковым.

В случае обнаружения файла, классифицированного как шпионская программа, рекомендуется удалить его, так как скорее всего он содержит вредоносный код.

15.1.7 Потенциально опасные приложения

Существует множество нормальных программ, предназначенных для упрощения администрирования подключенных к сети компьютеров. Однако злоумышленники могут использовать их для причинения вреда. ESET Cyber Security Pro позволяет выявлять такие угрозы.

Потенциально опасные приложения — это обычно коммерческое законное программное обеспечение. В эту категорию входят такие программы, как средства удаленного доступа, приложения для взлома паролей и клавиатурные шпионы (программы, записывающие нажатия клавиш на клавиатуре).

15.1.8 Потенциально нежелательные приложения

Потенциально нежелательные приложения не обязательно являются вредоносными, но могут отрицательно влиять на производительность компьютера. Такие приложения обычно запрашивают при установке согласие пользователя. После их установки работа системы изменяется. Наиболее заметны следующие изменения.

- Открываются новые окна, которые не появлялись ранее.
- Активируются и выполняются скрытые процессы.
- Повышается уровень потребления системных ресурсов.
- Появляются изменения в результатах поиска.
- Приложения подключаются к удаленным серверам.

15.2 Типы удаленных атак

Существует множество особых методов, с помощью которых злоумышленники могут подвергать опасности удаленные системы. Выделяют несколько категорий.

15.2.1 DoS-атаки

DoS-атака или атака типа «отказ в обслуживании» — это попытка сделать компьютер или сеть недоступными для непосредственных пользователей на некоторое время. Связь между пострадавшими пользователями блокируется и больше не может полноценно функционировать. Как правило, для возобновления нормальной работы компьютеров, которые подвергаются DoS-атакам, требуется выполнить их перезагрузку.

В большинстве случаев эти атаки направлены на то, чтобы на некоторое время сделать веб-серверы недоступными для пользователей.

15.2.2 Атака путем подделки записей кэша DNS

Атака путем подделки записей кэша DNS (сервер доменных имен) может позволить злоумышленникам заставить DNS-сервер любого компьютера использовать предоставляемые ими фиктивные сведения как законные и настоящие. Фиктивная информация некоторое время сохраняется в кэше, что позволяет злоумышленникам переписывать ответы DNS-сервера с IP-адресами. В результате при попытке зайти на какие-либо веб-сайты вместо оригинального содержимого пользователи будут загружать компьютерные вирусы или черви.

15.2.3 Сканирование портов

Сканирование портов используется для определения открытых портов на сетевом узле. Сканер портов — это программа, разработанная для поиска таких портов.

Порт компьютера является виртуальной точкой, на которой обрабатываются все входящие и исходящие данные и которая является важнейшим объектом, с точки зрения безопасности. В больших сетях информация, собранная при помощи сканеров портов, может способствовать выявлению потенциально слабых мест. Такое использование является законным.

Однако сканирование портов зачастую используется злоумышленниками для нарушения безопасности. Сначала они отправляют пакеты на каждый из портов. В зависимости от типа ответа можно определить, какие порты используются. Само по себе сканирование является безопасным, но с его помощью злоумышленники могут выявить уязвимые места и получить контроль над удаленными компьютерами.

Сетевым администраторам рекомендуется блокировать те порты, которые не используются, и обеспечить защиту используемых портов от несанкционированного доступа.

15.2.4 Десинхронизация TCP

Десинхронизация TCP — это метод, который используется при атаках TCP Hijacking. Она инициируется процессом, в котором порядковый номер входящих пакетов отличается от ожидаемого порядкового номера. Пакеты с непредусмотренным порядковым номером пропускаются (или сохраняются в буфере, если они присутствуют в текущем окне подключения).

При десинхронизации оба подключенных компьютера отклоняют полученные пакеты; на этом этапе удаленные злоумышленники могут внедрять и предоставлять пакеты с правильным порядковым номером. Злоумышленники могут даже управлять подключением или изменять его.

Целью атак TCP Hijacking является прерывание подключений сервер-клиент или одноранговых подключений. Многих атак можно избежать благодаря использованию аутентификации для каждого сегмента TCP. Также следует использовать рекомендованную конфигурацию для сетевых устройств.

15.2.5 SMB Relay

SMBRelay и SMBRelay2 — это специальные программы, которые могут осуществлять атаки против удаленных компьютеров. Эти программы используют протокол совместного доступа к файлам SMB на основе NetBIOS. Пользователь, предоставляющий общий доступ к какой-либо папке или каталогу в локальной сети, вероятнее всего, использует этот протокол совместного доступа к файлам.

В рамках подключения по локальной сети происходит обмен хэшами паролей.

Программа SMBRelay получает подключение на портах UDP 139 и 445, ретранслирует пакеты, которыми обмениваются клиент и сервер, и изменяет их. После подключения и аутентификации клиент отключается. SMBRelay создает новый виртуальный IP-адрес. SMBRelay ретранслирует обмен данными по протоколу SMB, за исключением согласования и аутентификации. Удаленные злоумышленники могут использовать IP-адрес на протяжении всего времени подключения клиентского компьютера.

SMBRelay2 работает по тому же принципу, что и SMBRelay, но использует имена NetBIOS, а не IP-адреса. Обе программы могут осуществлять атаки «злоумышленник в середине». Эти атаки позволяют удаленным злоумышленникам незаметно читать, вставлять и изменять сообщения, которыми обмениваются два подключенных компьютера. Компьютеры, которые подвергаются таким атакам, часто перестают отвечать на запросы или неожиданно выполняют перезагрузку.

Чтобы избежать таких атак, рекомендуется использовать пароли или ключи для аутентицикации.

15.2.6 Атаки по протоколу ICMP

Протокол ICMP — это популярный и широко распространенный интернет-протокол. Он используется в основном для отправки сетевыми компьютерами различных сообщений об ошибках.

Злоумышленники пытаются использовать уязвимость в протоколе ICMP. Протокол ICMP разработан для односторонней передачи данных, для которой не требуется аутентификация. Поэтому злоумышленники могут осуществлять атаки типа «отказ в обслуживании» (DoS-атаки) или атаки, в результате которых можно получить несанкционированный доступ к входящим и исходящим пакетам.

Типичными примерами атак по протоколу ICMP являются атака ping flood, атака ICMP_ECHO flood и атака Smurf. Скорость работы компьютеров, которые подвергаются атакам по протоколу ICMP, существенно уменьшается (это относится ко всем приложениям, которые используют Интернет). Кроме того, возникают проблемы с подключением к Интернету.

15.3 Электронная почта

Электронная почта — это современная форма общения со множеством преимуществ. Это гибкий, быстрый и прямой способ общения, который сыграл решающую роль в распространении Интернета в начале 90-х.

К сожалению, из-за высокой степени анонимности электронная почта и Интернет открывают возможности для такой незаконной деятельности, как рассылка спама. К спаму относятся незапрошенные рекламные сообщения, письма-мистификации и распространение вредоносных программ. Уровень опасности и причиняемого неудобства еще более высок, поскольку стоимость отправки спама минимальна, а у его создателей есть множество средств для получения новых адресов электронной почты. Кроме того, очень сложно контролировать спам из-за его разновидностей и масштабов рассылки. Чем дольше используется адрес электронной почты, тем больше вероятность того, что он окажется в базе данных системы рассылки спама. Несколько советов о том, как этого избежать:

- постарайтесь не афишировать свой адрес электронной почты в Интернете;
- сообщайте свой адрес электронной почты только тем, кому доверяете;
- постарайтесь не использовать распространенные имена пользователей — чем сложнее имя пользователя, тем меньше вероятность того, что оно будет угадано;
- не отвечайте на спам-сообщения, которые попадают в ваш почтовый ящик;
- будьте бдительны при заполнении различных форм в Интернете — обращайте особое внимание на такие поля, как *Да, я хочу получат ь информацию*;
- заведите «специализированные» адреса электронной почты: один — для работы, другой — для общения с друзьями и т. д.;
- время от времени меняйте свой адрес электронной почты;
- используйте средство защиты от спама.

15.3.1 Рекламные сообщения

Реклама в Интернете — одна из наиболее быстро развивающихся форм рекламы. Главными маркетинговыми преимуществами такой рекламы являются ее минимальная стоимость, высокая степень направленности и, что более важно, практически мгновенная доставка сообщений. Многие компании используют средства электронного маркетинга для эффективного общения со своими существующими и

потенциальными пользователями.

Данный тип рекламы является законным, поскольку вы можете быть заинтересованы в получении коммерческой информации о некоторых продуктах. Но многие компании практикуют массовые отправки незапрошенных коммерческих сообщений. В этом случае рекламные сообщения электронной почты выходят за допустимые рамки и превращаются в спам.

Масштаб рассылки незапрошенных сообщений стал проблемой, решения для которой пока не существует. Создатели нежзапрошенных сообщений зачастую стараются замаскировать спам, чтобы выдать его за обычные сообщения.

15.3.2 Письма-мистификации

Письмо-мистификация — это ложная информация, которая распространяется в сети Интернет. Письма-мистификации обычно распространяются с помощью электронной почты или таких средств общения, как ICQ и Skype. Само по себе сообщение зачастую является шуткой или городской легендой.

Письма-мистификации о компьютерных вирусах направлены на то, чтобы вызвать у получателей страх, неуверенность и сомнение (FUD), заставить их поверить в существование вируса, который невозможно обнаружить и который уничтожает файлы, крадет пароли или другим способом вредит их компьютеру.

В некоторых письмах-мистификациях получателей просят переслать сообщение своим контактам, таким образом увеличивая срок существования подобных сообщений. Существуют также письма-мистификации для мобильных телефонов, просьбы о помощи, письма от людей, которые предлагают выслать вам деньги из-за границы и т. д. Определить намерения авторов таких сообщений зачастую невозможно.

Если вы получили сообщение, в котором вас просят переслать его всем своим знакомым, это наверняка письмо-мистификация. В Интернете существует множество веб-сайтов, с помощью которых можно проверить законность электронных сообщений. Перед тем как пересылать какое-либо сообщение, которое кажется вам подозрительным, выполните по нему поиск в Интернете.

15.3.3 Фишинг

Термином «фишинг» обозначается преступная деятельность с использованием социотехники (манипулирование пользователями для получения конфиденциальной информации). Эта деятельность направлена на получение такой конфиденциальной информации, как номера банковских счетов, PIN-коды и т. д.

Для получения этой информации электронные сообщения, как правило, отправляются от имени людей или компаний, которые вызывают доверие (финансовые учреждения, страховые компании и т. д.). Электронное сообщение может выглядеть так же, как настоящее, и включать в себя содержимое и графические средства, которые изначально могли использоваться тем же источником, которым теперь прикрываются мошенники. Вас под разными предлогами (проверка данных, финансовые операции) просят указать некоторые персональные данные: номера банковских счетов, имена пользователей и пароли. Если сообщить эту информацию, она может быть украдена или использована ненадлежащим образом.

Банки, страховые компании и прочие законопослушные организации никогда не запрашивают имена пользователей и пароли с помощью незапрошенных сообщений.

15.3.4 Распознавание спама

Существует несколько индикаторов для распознавания спама (незапрошенных сообщений) в вашем почтовом ящике. Сообщение вероятнее всего является спамом, если оно отвечает хотя бы некоторым из следующих критериев.

- Адреса отправителя нет в вашей адресной книге.
- Вам предлагают большую сумму денег, если вы сначала сделаете небольшой взнос.
- Вас под разными предлогами (проверка данных, финансовые операции) просят указать некоторые персональные данные, например номера банковских счетов, имена пользователей, пароли и т. д.
- Письмо написано на иностранном языке.
- Вам предлагают купить продукт, который вас не интересует. Если вы все-таки решились на покупку, удостоверьтесь, что отправитель сообщения является надежным поставщиком (это можно уточнить у производителя продукта).
- Некоторые слова написаны неправильно, чтобы обойти фильтр спама. Например, *vaigra* вместо *viagra* и т. д.