CYBER SECURITY

# ДЛЯ УСТРОЙСТВ MAC

## 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. 17. 10. 2013

# Содержание


1. ESET Cyber Security ..... 4
1.1 Новые возможности ..... 4
1.2 Системные требования ..... 4
2. Установка ..... 4
2.1 Обычная установка ..... 4
2.2 Выборочная установка ..... 5
3. Активация программы ..... 5
4. Удаление программы ..... 6
5. Основные сведения ..... 6
5.1 Сочетания клавиш ..... 6
5.2 Проверка состояния защиты ..... 6
5.3 Действия, которые следует выполнить, если программа не работает надлежащим образом ..... 6
6. Защита компьютера ..... 7
6.1 Защита от вирусов и шпионских программ ..... 7
6.1.1 Общие ..... 7
6.1.1.1 Исключения ..... 7
6.1.2 Защита при запуске ..... 7
6.1.3 Защита файловой системы в режиме реального времени ..... 8
6.1.3.1 Сканировать при (сканирование при определенных условиях) ..... 8
6.1.3.2 Расширенные параметры ..... 8
6.1.3.3 Изменение конфигурации защиты в режиме реального времени ..... 8
6.1.3.4 Проверка защиты в режиме реального времени ..... 8
6.1.3.5 Действия, которые следует выполнить, если модуль защиты в режиме реального времени не работает ..... 9
6.1.4 Сканирование компьютера по требованию ..... 9
6.1.4.1 Тип сканирования ..... 9
6.1.4.1.1 Сканирование Smart ..... 9
6.1.4.1.2 Выборочное сканирование ..... 9
6.1.4.2 Объекты сканирования ..... 10
6.1.4.3 Профили сканирования ..... 10
6.1.5 Настройка параметров модуля ThreatSense ..... 10
6.1.5.1 Объекты ..... 11
6.1.5.2 Параметры ..... 11
6.1.5.3 Очистка ..... 11
6.1.5.4 Расширения ..... 11
6.1.5.5 Ограничения ..... 12
6.1.5.6 Другие ..... 12
6.1.6 Действия при обнаружении заражения ..... 12
6.2 Сканирование и блокирование съемных носителей ..... 13
7. Защита от фишинга ..... 13
8. Защита доступа в Интернет и электронной почты ..... 13
8.1 Защита доступа в Интернет ..... 13
8.1.1 Порты ..... 13
8.1.2 Активный режим ..... 14
8.1.3 Списки URL-адресов ..... 14
8.2 Защита электронной почты ..... 14
8.2.1 Проверка протокола POP3 ..... 14
8.2.2 Проверка протокола IMAP ..... 15
9. Обновление ..... 15
9.1 Настройка обновления ..... 15
9.2 Создание задач обновления ..... 15
9.3 Обновление ESET Cyber Security до новой версии ..... 16
9.4 Обновления системы ..... 16
10. Сервис ..... 16
10.1 Файлы журнала ..... 16
10.1.1 Обслуживание журнала ..... 17
10.1.2 Фильтрация журнала ..... 17
10.2 Планировщик ..... 17
10.2.1 Создание новых задач ..... 18
10.2.2 Создание пользовательских задач ..... 18
10.3 Карантин ..... 18
10.3.1 Помещение файлов на карантин ..... 18
10.3.2 Восстановление из карантина ..... 19
10.3.3 Отправка файла из карантина ..... 19
10.4 Запущенные процессы ..... 19
10.5 Live Grid ..... 19
10.5.1 Настройка Live Grid ..... 20
10.6 ESET Social Media Scanner ..... 20
11. Интерфейс пользователя ..... 20
11.1 Предупреждения и уведомления ..... 20
11.1.1 Расширенные параметры предупреждений и уведомлений ..... 21
11.2 Разрешения ..... 21
11.3 Контекстное меню ..... 21
12. Разное ..... 21
12.1 Импорт и экспорт параметров ..... 21
12.1.1 Импорт параметров ..... 22
12.1.2 Экспорт параметров ..... 22
12.2 Настройка прокси-сервера ..... 22
13. Глоссарий ..... 22
13.1 Типы заражений ..... 22
13.1.1 Вирусы ..... 22
13.1.2 Черви ..... 22
13.1.3 Троянские программы ..... 23
13.1.4 Руткиты ..... 23
13.1.5 Рекламные программы ..... 23
13.1.6 Шпионские программы ..... 23
13.1.7 Потенциально опасные приложения ..... 24
13.1.8 Потенциально нежелательные приложения ..... 24
13.2 Типы удаленных атак ..... 24
13.2.1 DoS-атаки ..... 24
13.2.2 Атака путем подделки записей кэша DNS ..... 24
13.2.3 Сканирование портов ..... 24
13.2.4 Десинхронизация TCP ..... 25
13.2.5 SMB Relay ..... 25
13.2.6 Атаки по протоколу ICMP ..... 25
13.3 Электронная почта ..... 25
13.3.1 Рекламные сообщения ..... 26
13.3.2 Письма-мистификации ..... 26
13.3.3 Фишинг ..... 26
13.3.4 Распознавание спама ..... 26

# 1. ESET Cyber Security

ESET Cyber Security представляет собой новый подход к по-настоящему интегрированному обеспечению безопасности компьютера. Последняя версия модуля сканирования ThreatSense® характеризуется скоростью и точностью при обеспечении безопасности компьютера. Результатом является интеллектуальная система, которая постоянно готова к атакам и вредоносному программному обеспечению, которые угрожают компьютеру.

ESET Cyber Security — 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, способны обеспечить упреждающую защиту от вирусов, червей, троянских, шпионских и рекламных программ, руткитов и прочих интернет-атак, не ухудшая производительность системы и не нарушая работу компьютера.

## 1.1 Новые возможности

По сравнению с версией 5 программы ESET Cyber Security версия 6 содержит следующие обновления и улучшения.

**Защита от фишинга**
Данная функция предотвращает предоставление ваших личных данных фиктивным веб-сайтам, которые имитируют надежность.

**Интеграция приложения ESET Social Media Scanner**
Программа ESET Cyber Security связана с приложением, которое используется в социальных сетях для защиты учетных записей в Facebook и Твиттере от многочисленных угроз. Это приложение не зависит от других продуктов ESET и предоставляется на бесплатной основе.

**Обновления системы**
Версия 6 программы ESET Cyber Security исправляет различные проблемы и содержит улучшения, в том числе уведомления о доступных обновлениях для операционной системы Mac OS X 10.8. Чтобы узнать подробнее, см. раздел Обновления системы 16.

## 1.2 Системные требования

Для оптимальной работы ESET Cyber Security система должна отвечать перечисленным ниже аппаратным и программным требованиям.

| | Системные требования |
|---|---|
| Архитектура процессора | 32-разрядная или 64-разрядная Intel® |
| Операционная система | Mac OS X 10.6 или более поздней версии |
| Память | 300 Мб |
| Свободное место | 150 МБ |

# 2. Установка

Прежде чем приступать к процессу установки, нужно закрыть все открытые программы. ESET Cyber Security 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.

**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. По умолчанию флажок **Включить систему своевременного обнаружения Live Grid** установлен. Нажмите кнопку **Настройка...**, чтобы изменить детальные настройки отправки подозрительных файлов. Дополнительные сведения см. в разделе Live Grid 19.

**Особые 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 следует выполнить сканирование компьютера на предмет наличия вредоносного кода. В главном окне программы выберите пункт **Сканирование ПК**, 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 задать его параметры, установив флажок **Я использую прокси-сервер** . Далее введите IP-адрес или URL-адрес прокси-сервера в поле **Адрес**. В поле **Порт** укажите порт, по которому 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 прокси-сервер не используется, установите флажок **Я не использую прокси-сервер**. Если вы не уверены в выборе, можно использовать текущие системные параметры, установив флажок **Системные настройки (рекомендуется)**.

**Разрешения**
На следующем этапе можно определить пользователей с правами, которые смогут изменять конфигурацию программы. Для того чтобы наделить пользователей правами, выберите их в списке в левой части окна и нажмите кнопку **Добавить**. Чтобы отобразить всех системных пользователей, установите флажок **Показывать всех пользователей**. Если список "Пользователи с правами" пуст, все пользователи рассматриваются как обладатели прав.

**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. По умолчанию флажок **Включить систему своевременного обнаружения Live Grid** установлен. Нажмите кнопку **Настройка...**, чтобы изменить детальные настройки отправки подозрительных файлов. Дополнительные сведения см. в разделе Live Grid 19.

**Особые 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.

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

## 3. Активация программы

После установки на экране автоматически появится окно **Тип активации программы**. Или можно щелкнуть значок ESET Cyber Security, расположенный в строке меню (верхняя часть экрана), и выбрать вариант **Активация программы...**.

1. Если вы приобрели розничную упакованную версию программы, выберите вариант **Активировать с помощью ключа активации**. Ключ активации обычно находится внутри или на задней стороне упаковки программы. Для успешной активации ключ активации необходимо ввести так, как он указан на упаковке.

2. Если вы получили имя пользователя и пароль, выберите вариант **Активировать с помощью имени пользователя и пароля** и введите данные лицензии в соответствующие поля. Этот параметр соответствует параметру **Настройка имени пользователя и пароля...** в окне программы **Обновить**.

3. Если перед совершением покупки вы хотите оценить ESET Cyber Security, выберите вариант **Активировать пробную лицензию**. Укажите свой адрес электронной почты, чтобы активировать ESET Cyber Security на ограниченный период времени. Ваша пробная лицензия будет отправлена вам по электронной почте. Каждый пользователь может активировать только одну пробную лицензию.

Если активация в данный момент не требуется, нажмите кнопку **Активировать позднее**. Программу ESET Cyber Security можно активировать в разделе **Домашняя страница** или **Обновление** главного окна программы ESET Cyber Security.

Если у вас нет лицензии и вы хотите ее приобрести, выберите вариант **Лицензия**. В результате откроется веб-сайт местного распространителя ESET.

# 4. Удаление программы

Удалить ESET Cyber Security с компьютера можно одним из описанных ниже способов.

- Вставьте установочный компакт- или DVD-диск с программой ESET Cyber Security в дисковод, откройте его на рабочем столе или в окне **Finder** и дважды щелкните значок **Удалить**.
- Откройте установочный файл ESET Cyber Security (*DMG*-файл) и дважды щелкните значок **Удалить**.
- Запустите программу **Finder**, откройте папку **Приложения** на жестком диске, нажмите клавишу CTRL и щелкните значок **ESET Cyber Security**, а затем выберите команду **Показать содержимое пакета**. Откройте папку **Ресурсы** и дважды щелкните значок **Удалить**.

# 5. Основные сведения

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

Ниже описаны пункты главного меню.

- **Домашняя страница**: отображается информация о состоянии защиты компьютера, доступа в Интернет и электронной почты.
- **Сканирование компьютера**: этот пункт позволяет настроить и запустить сканирование компьютера по требованию 9.
- **Обновление**: выводит на экран информацию об обновлениях базы данных сигнатур вирусов.
- **Настройка**: этот пункт позволяет настроить уровень безопасности компьютера.
- **Сервис**: этот пункт предоставляет доступ к файлам журнала 16, планировщику 17, карантину 18, запущенным процессам 19 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.

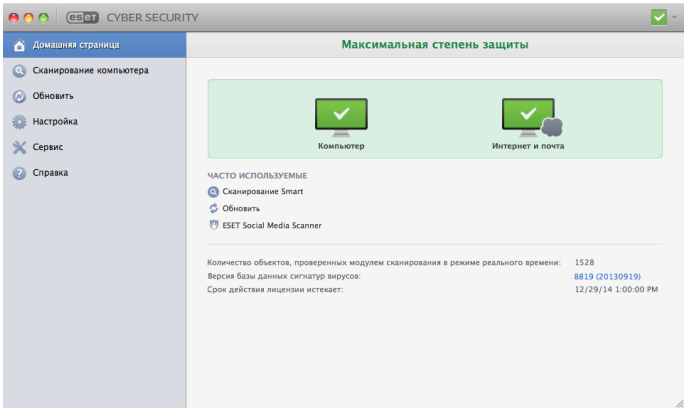
- *cmd+,*: отображаются настройки программы ESET Cyber Security.
- *cmd+U*: открывается окно **Настройка имени пользователя и пароля**.
- *cmd+alt+T*: открывается окно **Специальные символы**.
- *cmd+O* : позволяет восстановить размер по умолчанию главного окна программы ESET Cyber Security и переместить его в центр экрана.
- *cmd+alt+H* : скрывает все открытые окна, за исключением окна программыESET Cyber Security.
- *cmd+H*: позволяет скрыть окно программы ESET Cyber Security.

Нижеперечисленные сочетания клавиш работают, только если в меню **Настройка** > **Настроить параметры приложения...** включен параметр **Использовать обычное меню** (или нажмите *cmd+,*) > **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

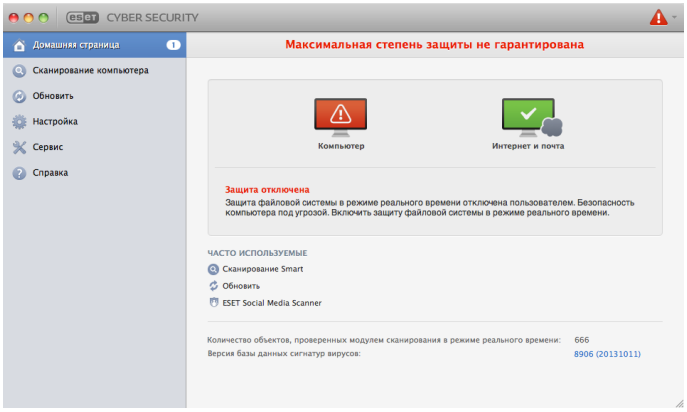
Чтобы просмотреть состояние защиты, выберите пункт **Домашняя страница** в главном меню. В основном окне появится сводная информация о работе модулей ESET Cyber Security.




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

Если включенные модули работают правильно, они обозначаются зеленым значком. Если же нет, появляется красный восклицательный знак или оранжевый значок уведомления. Отображаются дополнительные сведения об этом модуле и предлагается решение для устранения проблемы. Чтобы изменить состояние отдельных модулей, щелкните синюю ссылку внизу каждого уведомления.

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




# 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**. Учтите, 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

С помощью раздела **Исключения** можно исключить из сканирования определенные файлы, папки, приложения и адреса IP/IPv6.

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 не сканируется только на предмет этой угрозы, а не на предмет наличия угроз вообще. Если файл окажется заражен другой вредоносной программой, модуль защиты от вирусов ее обнаружит.
- **Добавить...**: команда, исключающая объекты из сканирования. Укажите путь к объекту (допускается использование подстановочных знаков * (звездочка) и ? (знак вопроса)) либо выберите папку или файл в структуре дерева.
- **Изменить...**: команда, позволяющая изменить выделенные записи.
- **Удалить**: команда, удаляющая выделенные записи.
- **По умолчанию**: команда, отменяющая все исключения.

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. При обработке новых файлов могут применяться углубленные способы контроля.

По умолчанию 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, нажав значок ESET Cyber Security, расположенный в строке меню (в верхней части экрана) и выбрав вариант **Отключить защиту файловой системы в режиме реального 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**).

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** (описание приведено в разделе Расширенные параметры сканирования 8).

#### 6.1.3.1 Сканировать при (сканирование при определенных условиях)

По умолчанию все файлы сканируются при их открытии, создании и исполнении. Рекомендуется не изменять параметры по умолчанию, поскольку они обеспечивают максимальную защиту компьютера в режиме реального времени.

#### 6.1.3.2 Расширенные параметры

В этом окне можно определить типы объектов для сканирования модулем ThreatSense, включить или отключить **расширенную эвристику**, а также изменить параметры для работы с архивами и файловым кэшем.

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

Можно включить или отключить сканирование ThreatSense с применением расширенной эвристики по отдельности для запущенных, созданных и измененных файлов, установив флажок **Расширенная эвристика** в соответствующих разделах параметров модуля ThreatSense .

Для того чтобы свести к минимуму влияние на производительность компьютера при использовании защиты в режиме реального времени, можно задать размер кэша оптимизации. Эта функция активна, если установить флажок **Включить очистку файлового кэша**. Если же он снят, все файлы сканируются каждый раз при доступе к ним. Файлы не будут сканироваться повторно после кэширования, если они не были изменены, пока не превышен указанный размер кэша. Файлы сканируются повторно сразу после каждого обновления базы данных сигнатур вирусов. Для того чтобы включить или отключить эту функцию, используйте флажок **Включить очистку файлового кэша**. Для задания количества кэшируемых файлов введите нужное значение в поле ввода **Размер кэша**.

В окне **Настройка модуля ThreatSense** можно настроить дополнительные параметры сканирования. например можно определить типы **объектов**, которые необходимо сканировать, используемые **параметры** и уровень **очистки**, а также указать **расширения** и **ограничения** размера файлов для защиты в режиме реального времени. Окно настройки модуля ThreatSense можно открыть, нажав кнопку **Настройка...** рядом с элементом **Модуль ThreatSense** в окне расширенной настройки. Дополнительные сведения о параметрах модуля ThreatSense см. в разделе Настройка параметров модуля ThreatSense 10.

#### 6.1.3.3 Изменение конфигурации защиты в режиме реального времени

Защита в режиме реального времени является наиболее важным элементом обеспечения безопасности системы. Изменять параметры модуля защиты в режиме реального времени следует с осторожностью. Рекомендуется делать это только в особых случаях, например при возникновении конфликтов с какими-либо приложениями или модулями сканирования в режиме реального времени других программ защиты от вирусов.

После установки ESET Cyber Security 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** (диалоговое окно **Настройка** > **Ввести настройки приложения...** > **Защита в режиме реального времени**).

#### 6.1.3.4 Проверка защиты в режиме реального времени

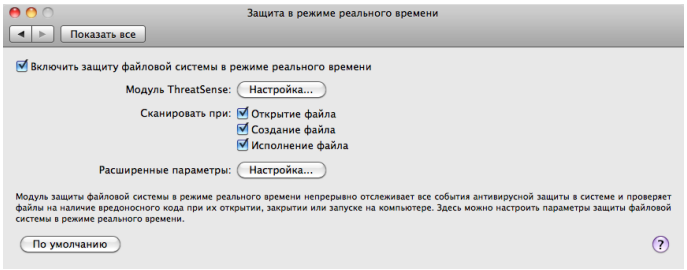
Чтобы убедиться в том, что защита в режиме реального времени работает и обнаруживает вирусы, воспользуйтесь тестовым файлом eicar.com. Это специальный безвредный файл, обнаруживаемый всеми программами защиты от вирусов. Он создан институтом EICAR (Европейский институт антивирусных компьютерных исследований)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

тестирования функциональности программ защиты от вирусов.

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

В этом разделе описаны проблемы, которые могут возникнуть при защите в режиме реального времени, и способы их устранения.

**Защита в режиме реального времени отключена**
Если защита в режиме реального времени была 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**. Или 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**.



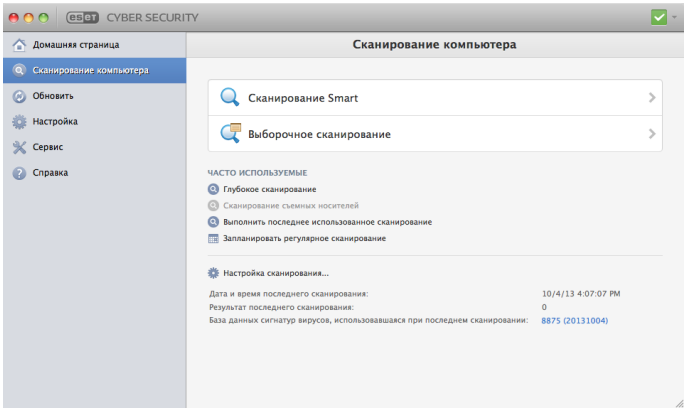

**Функция защиты в режиме реального времени не обнаруживает и не очищает заражения**
Убедитесь, что на компьютере не установлены другие программы защиты от вирусов. При одновременной работе двух систем защиты в режиме реального времени могут возникать конфликты. Рекомендуется удалить все другие программы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

### 6.1.4 Сканирование компьютера по требованию

При обнаружении симптомов возможного заражения компьютера (необычное поведение и т. п.) запустите сканирование ПК, воспользовавшись командами **Сканирование ПК** > **Сканирование Smart**. Для обеспечения максимальной защиты сканирование ПК 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**.




Также можно перетаскивать выделенные файлы и папки с рабочего стола или из окна **Finder** на основной экран ESET Cyber Security, 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 ПК 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, которые полезны, если сканирование с одинаковыми параметрами выполняется регулярно.

Чтобы указать объекты сканирования, выберите пункт **Сканирование ПК** > **Выборочное сканирование** и выделите нужные **объекты сканирования** в древовидной структуре. Объекты сканирования также можно задать более точно, указав пути к папкам и файлам, которые нужно сканировать. Если нужно только выполнить сканирование системы без выполнения дополнительных действий по очистке, установите флажок **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

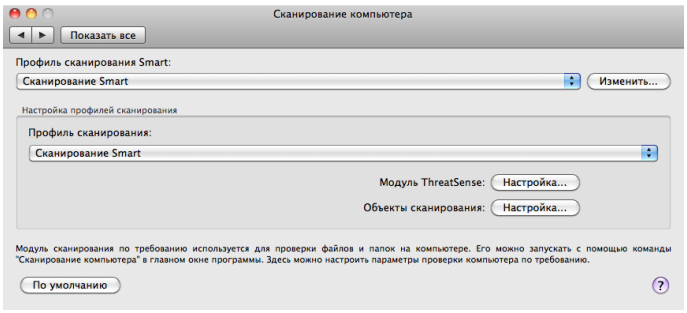
Древовидная структура объектов сканирования позволяет выбрать файлы и папки, которые необходимо просканировать на наличие вирусов. Выбор папок может также осуществляться в соответствии с параметрами профиля.

Объекты сканирования можно определить более точно, введя путь к папкам или файлам, подлежащим сканированию. Выберите объекты сканирования в древовидной структуре, содержащей все доступные на компьютере 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**.

### 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.

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.

- **Файлы**: сканируются файлы всех часто используемых типов (программы, изображения, звуковые и видеофайлы, файлы баз данных и т. д.).
- **Символические ссылки**: сканируются файлы особого типа, содержащие текстовую строку, которая интерпретируется и используется операционной системой как путь к другому файлу или каталогу (только для модуля сканирования по требованию).
- **Почтовые файлы**: сканируются особые файлы, содержащие сообщения 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**: сканируются программы-упаковщики, которые в отличие от стандартных архивов распаковывают файлы в системную память, и стандартные статические упаковщики (UPX, yoda, ASPack, FGS и т. д.).

#### 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.
- Система своевременного обнаружения **ESET Live Grid** помогает немедленно и беспрерывно информировать компанию ESET о новых заражениях для быстрой защиты клиентов. Дополнительные сведения см. в разделе Live Grid 19.

#### 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 файлы невозможно очистить, на экран выводится предупреждение с предложением выбрать действие.

***Предупреждение.*** В режиме стандартной очистки, который используется по умолчанию, архив удаляется целиком только в том случае, если все файлы в нем заражены. Если в архиве есть нормальные файлы, он не удаляется. Если зараженный архивный файл обнаруживается в режиме тщательной очистки, архив удаляется целиком, даже если в нем есть незараженные файлы.

#### 6.1.5.4 Расширения

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 **Добавить** и **Удалить** можно включать и запрещать сканирование для тех или иных расширений.

Иногда может быть необходимо исключить файлы из сканирования, если сканирование определенных типов файлов препятствует нормальной работе программы. Например, иногда целесообразно исключить из сканирования файлы с расширениями *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 установки этого ограничения модуль защиты от вирусов будет проверять только объекты меньше указанного размера. Не рекомендуется изменять значение по умолчанию, так как обычно это не нужно. 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 ESET постоянно вносит в нее изменения, которые можно интегрировать в ESET Cyber Security 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, представляют собой связи между файлами и папками, которые не видны для обычных методов 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.).

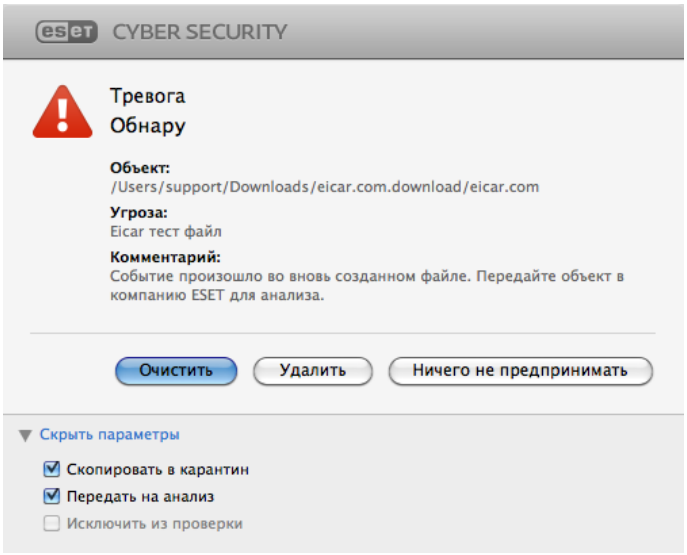
Если наблюдаются признаки заражения компьютера (например, он стал медленнее работать, часто «зависает» и т. п.), рекомендуется выполнить действия, описанные ниже.

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 предмет наличия вирусов.

Ниже описано, что происходит, когда система ESET Cyber Security выявляет заражение. Предположим, что заражение обнаружено модулем защиты файловой системы в режиме реального времени при уровне очистки по умолчанию. Сначала модуль 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 на компьютере. Исключением может быть ситуация, когда имеется полная уверенность в том, что файл безвреден и попал под подозрение по ошибке.

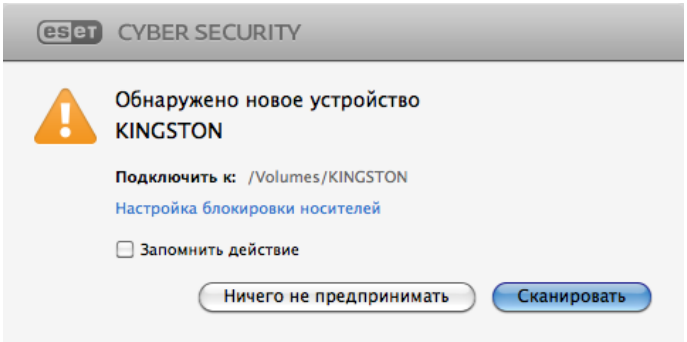
**Очистка и удаление.** Используйте очистку, если файл был атакован вирусом, добавившим в него вредоносный код. В этом случае в первую очередь следует попытаться очистить файл, чтобы восстановить его первоначальное состояние. Если файл содержит только вредоносный код, его следует удалить.




**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 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 выберите **Настройка** > **Ввести настройки приложения...** > **Носитель** в главном окне программы 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. Защита доступа в Интернет и электронной почты

Чтобы открыть раздел «Защита доступа в Интернет и электронной почты», в главном меню выберите пункт **Настройка** > **Интернет и электронная 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.

**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.

### 8.1 Защита доступа в Интернет

Функция защиты доступа в Интернет отслеживает обмен данными между веб-браузерами и удаленными серверами и соответствует правилам HTTP (протокола передачи гипертекста).

#### 8.1.1 Порты

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

### 8.1.2 Активный режим

ESET Cyber Security также содержит подменю **Активный режим**, которое определяет режим проверки для браузеров. Активный режим в целом анализирует данные, передаваемые приложениями, имеющими доступ к Интернету, независимо от того, отмечены они как браузеры или нет. Если этот параметр не включен, трафик приложений отслеживается постепенно, по пакетам. Это снижает эффективность процесса проверки данных, но и обеспечивает более высокую совместимость для приложений из списка. Если при использовании активного режима не возникают ошибки, рекомендуется включить активный режим проверки, установив флажок рядом с необходимым приложением.

Когда контролируемое приложение загружает данные, то сначала они сохраняются во временном файле, который создается программой ESET Cyber Security. Данные будут недоступны для такого приложения в данный момент. После завершения загрузки выполняется проверка на наличие вредоносного кода. Если заражение не обнаружено, данные отправляются в исходное приложение. Этот процесс обеспечивает полный контроль подключений, выполняемых контролируемым приложением. При активации пассивного режима данные постепенно загружаются в исходное приложение во избежание истечения времени ожидания.

### 8.1.3 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.

Если необходимо разрешить доступ только к URL-адресам из списка **Разрешенный URL-адрес**, выберите параметр **Ограничить URL-адреса**.

Чтобы активировать список, установите флажок **Включено**. 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.

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

После проверки сообщения в него добавляется уведомление с результатами сканирования. Можно выбрать параметр **Добавить уведомление к теме сообщений электронной почты**. На эти уведомления нельзя полагаться абсолютно, поскольку они могут быть пропущены в проблематичных сообщениях в формате HTML или фальсифицированы некоторыми вирусами. Доступны указанные ниже настройки.

**Никогда**: уведомления не добавляются.
**Только в зараженные сообщения**: помечаются как проверенные только сообщения, содержащие вредоносные программы.
**Во все просканированные сообщения электронной почты** : программа добавляет уведомления во все просканированные сообщения.

**Шаблон добавления к теме зараженных писем**: отредактируйте этот шаблон, если требуется изменить формат префикса темы для зараженных писем.

**Добавить уведомление к сноске сообщений электронной почты**: 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.

### 8.2.1 Проверка протокола POP3

Протокол POP3 является самым распространенным протоколом, используемым для получения сообщений в клиентских приложениях для работы с электронной почтой. ESET Cyber Security 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. Для правильной работы модуля убедитесь, что он включен. Контроль протокола POP3 осуществляется автоматически без необходимости перенастройки 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.

### 8.2.2 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 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. Для правильной работы модуля убедитесь, что он включен. Контроль протокола IMAP осуществляется автоматически без необходимости перенастройки 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.

# 9. Обновление

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

Выбрав пункт **Обновление** в главном меню, можно получить информацию о текущем состоянии обновления, в том числе дату и время последнего успешно выполненного обновления, а также сведения о необходимости обновления. Чтобы вручную запустить процесс обновления, нажмите **Обновить базу данных сигнатур вирусов**.

Обычно после корректного завершения загрузки в окне обновления выводится сообщение **База данных сигнатур вирусов актуальна**. Если обновить базу данных сигнатур вирусов невозможно, рекомендуется проверить настройки обновления 15, так как самая распространенная причина этой ошибки — неверно введенные данные для аутентификации (имя пользователя и пароль) или некорректно выбранные параметры подключения 22.

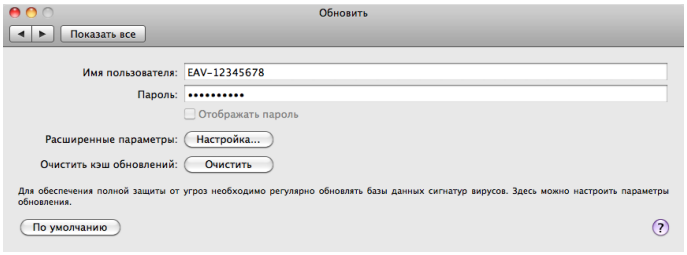
В окне обновления также выводятся сведения о версии базы данных сигнатур вирусов. Этот числовой индикатор представляет собой активную ссылку на веб-сайт ESET со списком всех сигнатур, добавленных во время текущего обновления.

**ПРИМЕЧАНИЕ.** Имя пользователя и пароль предоставляются компанией ESET после приобретения ESET Cyber Security.

## 9.1 Настройка обновления

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

Чтобы включить тестовый режим (для загрузки тестовых обновлений), выберите **Настройка** > **Ввести настройки приложения...** (или нажмите *cmd+,*) > **Обновить**, нажмите кнопку **Настройка...** рядом с пунктом **Расширенные параметры** и установите флажок **Включить тестовые обновления**. При решении проблем с ESET Cyber Security тестовый режим рекомендуется использовать только в ситуациях, когда доступно тестовое обновление.




Для отключения уведомлений на панели задач после каждого успешно выполненного обновления установите флажок **Не отображать уведомление об успешном обновлении**.

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

## 9.2 Создание задач обновления

Обновление можно запустить вручную с помощью функции **Обновить базу данных сигнатур вирусов** в основном окне, которое выводится на экран после выбора пункта **Обновление** в главном меню.

Обновления также можно выполнять как запланированную задачу. Для конфигурирования запланированной задачи перейдите в раздел **Служебные программы** > **Планировщик**. По умолчанию в ESET Cyber Security 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 17.

### 9.3 Обновление ESET Cyber Security до новой версии

Для обеспечения максимальной защиты важно использовать новейшую сборку ESET Cyber Security. Чтобы проверить наличие новой версии, выберите пункт **Домашняя страница** в главном меню слева. 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 была нажата кнопка **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 с компакт- или DVD-диска.

### 9.4 Обновления системы

Функция обновления системы Mac OS X 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 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 оповещения отображаются общие сведения о доступных обновлениях для операционной системы Mac OS X 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, 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.

## 10. Сервис

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

### 10.1 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.

Получить доступ к файлам журнала можно из главного меню ESET Cyber Security, 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.
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.

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

### 10.1.1 Обслуживание журнала

Конфигурация журнала ESET Cyber Security 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.
- **Автоматически оптимизировать файлы журналов**: данный параметр включает функцию автоматической дефрагментации файлов журналов в случае превышения указанной процентной доли неиспользуемых записей.

Чтобы конфигурировать **фильтр записей журналов, заданный по умолчанию**, нажмите кнопку **Изменить...** и выберите нужные типы журналов.

### 10.1.2 Фильтрация журнала

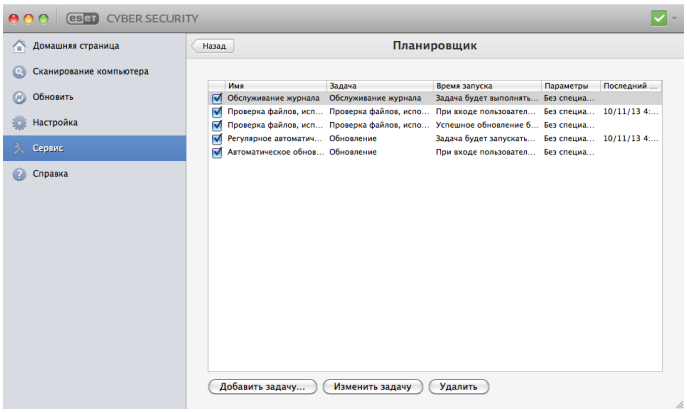
В журналах хранится информация о важных системных событиях. Функция фильтрации журнала позволяет отобразить записи о событиях определенного типа.

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.

## 10.2 Планировщик

**Планировщик** можно найти в главном меню ESET Cyber Security, воспользовавшись пунктом **Сервис**. **Планировщик** содержит полный список всех запланированных задач и их параметры запуска (дату, время и используемый профиль сканирования).




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

По умолчанию в планировщике отображаются следующие запланированные задачи:

- Обслуживание журнала (после установки флажка **Показывать системные задачи** при настройке планировщика)
- Проверка файлов при входе пользователя
- Проверка файлов 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**.

### 10.2.1 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 Mac OS X.

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 18).
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 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**.

### 10.2.2 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.

## 10.3 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 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 отправить в лабораторию ESET на анализ.

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. Файлы на карантине хранятся в безопасном зашифрованном виде. Их можно восстановить после повторной установки приложения ESET Cyber Security.

### 10.3.1 Помещение файлов на карантин

Программа ESET Cyber Security автоматически помещает удаленные файлы на карантин (если эта функция не была отключена пользователем в окне предупреждения). При желании любой подозрительный файл можно поместить на карантин вручную с помощью кнопки **Карантин...**. Для этого также можно использовать контекстное меню. Нажмите клавишу CTRL, щелкните мышью в пустом поле, выберите **Карантин**, выделите файл, который нужно поместить на карантин, и нажмите кнопку **Открыть**.

### 10.3.2 Восстановление из карантина

Файлы, находящиеся на карантине, можно восстановить в исходном месте. Для этого используется кнопка **Восстановить**. Функция восстановления также доступна в контекстном меню. Для ее использования нужно нажать клавишу CTRL, щелкнуть мышью нужный файл в окне «Карантин» и выбрать пункт **Восстановить**. Контекстное меню содержит также функцию **Восстановить в...**, которая позволяет восстановить файл в месте, отличном от исходного.

### 10.3.3 Отправка файла из карантина

Если на карантин помещен файл, угроза в котором не обнаружена программой, или файл неверно квалифицирован как зараженный (например, в результате эвристического анализа кода) и отправлен на карантин, передайте этот файл в лабораторию ESET. Для отправки помещенного на карантин файла нажмите клавишу CTRL, щелкните мышью нужный файл и в контекстном меню выберите **Отправить файл на анализ**.

## 10.4 Запущенные процессы

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

- **Процесс**: имя процесса, запущенного в настоящий момент на компьютере. Для просмотра всех запущенных процессов можно также использовать монитор активности (находится в папке */Applications/Utilities*).
- **Уровень риска**: в большинстве случаев программа ESET Cyber Security и технология ESET Live Grid присваивают уровни риска объектам (файлам, процессам и т. п.) с помощью ряда эвристических правил, которые проверяют характеристики каждого объекта, а затем оценивают их потенциальную способность к вредоносным действиям. На основании этого эвристического анализа объектам присваивается уровень риска. Известные приложения, 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 в файле, его можно отправить в лабораторию ESET для анализа. Если окажется, что файл является вредоносным, его обнаружение будет добавлено 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.

## 10.5 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**.

### 10.5.1 Настройка Live Grid

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

При обнаружении подозрительного файла его можно отправить в нашу лабораторию для анализа. Для этого в главном окне программы выберите **Сервис** > **Отправить файл на анализ**. Если это вредоносное приложение, его обнаружение будет добавлено в следующее обновление базы данных сигнатур вирусов.

**Отправка анонимной статистической информации**: система своевременного обнаружения ESET Live Grid собирает анонимную информацию о компьютере, связанную с новыми обнаруженными угрозами. Эта информация включает имя вредоносной программы, дату и время ее обнаружения, версию приложения ESET, версию операционной системы компьютера и информацию о его расположении. Как правило, статистическая информация поступает 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.

## 10.6 ESET Social Media Scanner

Приложение ESET Social Media Scanner защищает вас от вредоносного содержимого, распространяемого через социальные сети. Программа отслеживает содержимое, которое появляется в социальных сетях (например, публикуемые на стене Facebook ссылки и мультимедийные материалы) и обнаруживает вредоносный код в результате автоматического сканирования и сканирования по требованию. Отчет о результатах сканирования предоставляется пользователю в виде сообщения внутри самого приложения, а также по электронной почте или в качестве комментария в отношении зараженного объекта. Еженедельная статистика публикуется на стене пользователя в целях обеспечения его безопасности от угроз. Приложение ESET Social Media Scanner не зависит от других продуктов ESET для обеспечения безопасности и предоставляется на бесплатной основе.

Чтобы перейти на веб-страницу ESET Social Media Scanner и загрузить приложение, в главном меню программы ESET Cyber Security выберите пункт **Служебные программы** > **ESET Social Media Scanner**.

# 11. 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 при запуске системы установите флажок **Показывать заставку при запуске**.

С помощью параметра **Поместить приложение на панель Dock** можно разместить значок ESET Cyber Security на панели Dock ОС Mac OS, а также переключаться между программой ESET Cyber Security и другими запущенными приложениями с помощью сочетания клавиш *cmd-tab*. Изменения вступают в силу после повторного запуска программы ESET Cyber Security (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 Mac OS (в верхней части экрана).

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

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

## 11.1 Предупреждения и уведомления

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

Если снять флажок **Отображать предупреждения**, предупреждения выводиться не будут, поэтому делать это без особых причин не рекомендуется. В большинстве случаев рекомендуется оставить для этого параметра значение по умолчанию (флажок установлен).

Флажок **Отображать уведомления на рабочем столе**

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

Если при выполнении приложений в полноэкранном режиме требуется отображать только уведомления, требующие вмешательства пользователя, установите флажок **Включить полноэкранный режим**. Эта функция полезна при проведении презентаций, в компьютерных играх и при выполнении других задач, при которых задействован весь экран целиком.

#### 11.1.1 Расширенные параметры предупреждений и уведомлений

В ESET Cyber Security отображаются диалоговые окна с предупреждениями, которые информируют пользователя о новых версиях программы, новых обновлениях ОС, отключении определенных компонентов программы, удалении журналов и т. д. Каждое подобное уведомление можно отключить, установив флажок **Больше не показывать это диалоговое окно** в каждом диалоговом окне.

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

### 11.2 Разрешения

Параметры программы ESET Cyber Security 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**. Для того чтобы удалить пользователя, выберите его имя в списке **Пользователи с правами** в правой части окна и нажмите кнопку **Удалить**.

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

### 11.3 Контекстное меню

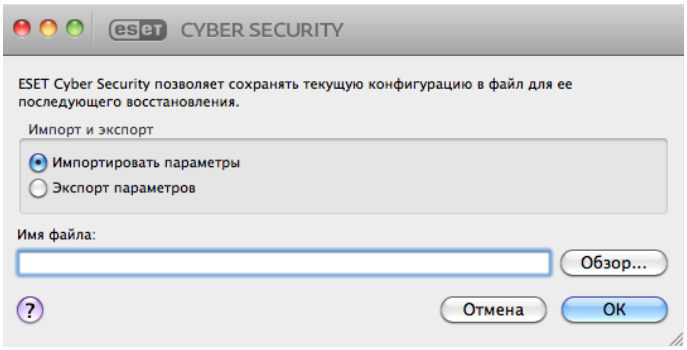
Для того чтобы включить интеграцию элементов в контекстное меню, щелкните **Настройка** > **Настроить параметры приложения...** (или нажмите *cmd+,*) > **Контекстное меню**, установив флажок **Интегрировать с контекстным меню**. Чтобы изменения вступили в силу, необходимо выйти из системы или перезагрузить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

## 12. Разное

### 12.1 Импорт и экспорт параметров

Импорт и экспорт конфигураций программы ESET Cyber Security можно выполнить с помощью панели **Настройка**.

Для хранения конфигурации при импорте и экспорте используются файлы архивов. Импорт и экспорт удобны, если нужно создать резервную копию текущей конфигурации ESET Cyber Security для дальнейшего использования. Экспорт параметров также полезен, если необходимо использовать выбранную конфигурацию ESET Cyber Security на нескольких системах, поскольку файл конфигурации можно легко импортировать для переноса нужных настроек.



#### 12.1.1 Импорт параметров

Для экспорта конфигурации выберите в главном меню **Настройка** > **Импорт и экспорт параметров...**, а затем выберите параметр **Импортировать параметры**. Введите имя файла конфигурации или нажмите кнопку **Обзор...**, чтобы выбрать файл, который необходимо импортировать.

#### 12.1.2 Экспорт параметров

Для экспорта конфигурации выберите в главном меню **Настройка** > **Импорт и экспорт параметров...**. Выберите пункт **Экспорт параметров** и введите имя файла конфигурации. С помощью проводника выберите место на компьютере для сохранения файла конфигурации.

### 12.2 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. Они используются всеми модулями программы, которым требуется подключение к Интернету. ESET Cyber Security 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).

Если для связи с прокси-сервером требуется аутентификация, установите флажок **Прокси-сервер требует аутентификации**, а затем в соответствующих полях укажите действительные **имя пользователя** и **пароль**.

## 13. Глоссарий

### 13.1 Типы заражений

Под заражением понимается вредоносная программа, которая пытается проникнуть на компьютер пользователя и (или) причинить ему вред.

#### 13.1.1 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 атакуют в основном 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. С другой стороны, некоторые вирусы не причиняют никакого вреда. Они просто раздражают пользователя и демонстрируют 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, т. е. очистить их с помощью программы защиты от вирусов.

#### 13.1.2 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 реплицироваться и распространяться самостоятельно, так как 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 считаные 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 зараженные файлы, поскольку они с большой вероятностью содержат злонамеренный код.

### 13.1.3 Троянские программы

Исторически троянскими программами называют особую группу заражений, 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.

- Загрузчик — вредоносная программа, которая загружает другие заражения из Интернета.
- Dropper — тип троянских программ, разработанных для заражения компьютеров другими вредоносными программами.
- Backdoor — 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 пользователю практически невозможно 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.

### 13.1.4 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.

Для предотвращения работы руткитов используются два уровня обнаружения.

1. Когда они пытаются попасть в систему. Они все еще вне системы, поэтому неактивны. Большинство антивирусных систем способно обезвредить руткиты на этом уровне (подразумевается, что такие файлы распознаются как зараженные).
2. Когда они скрыты от обычного тестирования.

### 13.1.5 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 пользователь решает использовать бесплатный программный продукт, ему следует уделить особое внимание установке. 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 часто 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 злонамеренный код.

### 13.1.6 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, могут служить клиенты пиринговых (P2P) сетей. Программы Spyfalcon и Spy Sheriff (и многие другие) относятся к особой подкатегории шпионских программ. Утверждается, что они предназначены для защиты от шпионских программ, но на самом деле сами являются таковыми.

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

#### 13.1.7 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 позволяет выявлять такие угрозы.

В качестве потенциально опасных приложений выступает нормальное коммерческое 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).

Если такая программа обнаружена на компьютере, но вы не устанавливали ее, обратитесь к администратору сети за консультацией или удалите ее.

#### 13.1.8 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.
- Приложение подключается к удаленным серверам.

### 13.2 Типы удаленных атак

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

#### 13.2.1 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.

#### 13.2.2 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.

#### 13.2.3 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.

#### 13.2.4 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 рекомендованные конфигурации для сетевых устройств.

#### 13.2.5 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, использующий какую-либо общую папку или каталог по 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.

#### 13.2.6 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.

### 13.3 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 надежным лицам;

- постарайтесь не использовать распространенные имена пользователей — чем сложнее имя пользователя, тем меньше вероятность, 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 получать 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 средства защиты от спама.

### 13.3.1 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.

### 13.3.2 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.

### 13.3.3 Фишинг

Термином «фишинг» обозначается преступная деятельность с использованием методов 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.

### 13.3.4 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.