

Norton™ Security

Руководство по продукту



Руководство по продукту Norton™ Security

Описанное в этом документе программное обеспечение поставляется с лицензионным соглашением, и его можно использовать только при соблюдении условий этого соглашения.

Версия документации: 8.5.4

© Symantec Corporation, 2020 г. Все права защищены.

Продукт, описанный в настоящем документе, распространяется на условиях лицензии, ограничивающей его использование, копирование, распространение, а также декомпиляцию или получение исходного кода. Запрещается полное или частичное воспроизведение настоящего документа любыми способами без предварительного письменного разрешения компании Symantec Corporation и ее лицензиаров, при наличии таковых.

ДАННАЯ ДОКУМЕНТАЦИЯ ПРЕДОСТАВЛЯЕТСЯ В ТОМ ВИДЕ, В КОТОРОМ ОНА СУЩЕСТВУЕТ НА ДАННЫЙ МОМЕНТ ("КАК ЕСТЬ"), С ОТКАЗОМ ОТ КАКИХ-ЛИБО УСЛОВИЙ, ПРЕДСТАВЛЕНИЙ И ГАРАНТИЙ, ЯВНЫХ ИЛИ ПОДРАЗУМЕВАЕМЫХ, ВКЛЮЧАЯ ПОДРАЗУМЕВАЕМЫЕ ГАРАНТИИ КОММЕРЧЕСКОЙ ЦЕННОСТИ, ПРИГОДНОСТИ ДЛЯ КАКОЙ-ЛИБО ЦЕЛИ, СОБЛЮДЕНИЯ ЧЬИХ-ЛИБО ПРАВ, ЗА ИСКЛЮЧЕНИЕМ ПРОТИВОРЕЧАЩИХ ДЕЙСТВУЮЩЕМУ ЗАКОНОДАТЕЛЬСТВУ. SYMANTEC CORPORATION НЕ МОЖЕТ НЕСТИ ОТВЕТСТВЕННОСТЬ ЗА СЛУЧАЙНОЕ ИЛИ НАМЕРЕННОЕ ПРИЧИНЕНИЕ УБЫТКОВ В СВЯЗИ С РАБОТОЙ ПРОДУКТА ИЛИ ИСПОЛЬЗОВАНИЕМ ЭТОЙ ДОКУМЕНТАЦИИ. ИНФОРМАЦИЯ, СОДЕРЖАЩАЯСЯ В НАСТОЯЩЕМ ДОКУМЕНТЕ, МОЖЕТ ИЗМЕНЯТЬСЯ БЕЗ ПРЕДВАРИТЕЛЬНОГО УВЕДОМЛЕНИЯ.

Лицензионное программное обеспечение и документация рассматриваются как коммерческое компьютерное программное обеспечение в соответствии с определением, данным в документе FAR 12.212, и подпадают под ограничение прав на использование в соответствии с разделами FAR 52.227-19 Commercial Computer Software - Restricted Rights и DFARS 227.7202 "Коммерческое программное обеспечение для компьютеров и документация по коммерческому программному обеспечению для компьютеров", в зависимости от применимых требований, а также иные нормативные акты, предоставленные компанией Symantec в соответствии с вышеуказанными или размещенными службами. Любое использование, видоизменение, воспроизведение, представление и распространение лицензируемого программного обеспечения и документации правительством США должно осуществляться исключительно в соответствии с условиями данного соглашения.

Symantec Corporation
350 Ellis Street,
Mountain View, CA 94043

<http://www.symantec.ru>

Оглавление

Глава 1	Вас приветствует Norton	6
	Начало работы с Norton для Mac	6
	Требования к системе для Norton Security	7
Глава 2	Загрузка и установка продукта Norton	8
	Загрузка и установка продукта Norton	8
	Установка продукта Norton на дополнительных устройствах	10
	Перенос лицензии Norton на новое устройство	12
	Активация или продление подписки на Norton для Mac	13
Глава 3	Описание угроз и реагирование на них	15
	Исправление, восстановление или удаление файлов, помещенных в карантин	15
	Запуск LiveUpdate для обновления Norton на Mac	16
Глава 4	Управление безопасностью	18
	Просмотр и настройка задач, которые Norton выполняет для защиты вашего Mac	18
	Просмотр или настройка сетевой активности, которую Norton отслеживает на вашем Mac	20
Глава 5	Сканирование компьютера Mac	22
	Сканирование Norton для проверки Mac на наличие угроз	22
	Настройка параметров автоматического сканирования Norton на Mac	24
	Планирование сканирования Norton на Mac	25
	Настройка сканирования вашего Mac во время простоя	25
Глава 6	Обеспечение безопасности в Интернете	27
	Защита от уязвимостей	28
	Настройте Брандмауэр Norton, чтобы запретить доступ к вашему Mac вредоносным веб-сайтам	28
	Выключение или включение защиты от уязвимостей	30

	Исключение или добавление сигнатур атаки на Mac	31
	Включение или выключение уведомлений о заблокированных сигнатурах атак на Mac	32
	Параметры брандмауэра для Mac	33
	Правило брандмауэра для IP-адресов на Mac	34
	Настройка правил брандмауэра для IP-адреса на Mac	35
	Изменение правил брандмауэра для IP-адреса на Mac	36
	Удаление правила брандмауэра для IP-адреса на Mac	37
	Расширенная защита для Mac	38
	Выключение или включение компонентов расширенной защиты на Mac	38
	Настройка загрузки данных из сообщества Norton DeepSight на Mac	39
	Настройка параметров автоматической блокировки на Mac	40
	Настройка параметров сигнатур на Mac	41
	Обновление до последней версии Norton для лучшей защиты вашего Mac	42
	Помогите Norton Community Watch определить новые потенциальные угрозы для Mac	44
	Отправка отчетов в Symantec при обнаружении программой Norton ошибки на Mac	45
Глава 7	Поддержание производительности компьютера Mac на высоком уровне	46
	Выполните сканирование Norton Clean для удаления файлов, которые снижают скорость работы вашего Mac	46
	Планирование или настройка сканирования Norton Clean для повышения скорости работы вашего Mac	47
Глава 8	Защита конфиденциальной информации	49
	Настройка Norton для обнаружения мошеннических или фишинговых веб-сайтов на Mac	49
	Добавьте расширение Norton в браузер, чтобы повысить безопасность работы и совершения онлайн-покупок на Mac	50
Глава 9	Настройка параметров	56
	Параметры блокировки соединения на Mac	57
	Настройка параметров блокировки соединения на Mac	57
	Параметры доступа для приложения	59
	Настройка параметров доступа для приложения	60

Параметры доступа для службы	62
Настройка параметров доступа для служб	63
Настройка особых параметров доступа для службы	65
Изменение параметров доступа для службы	66
Удаление параметров доступа для службы	68
Настройка брандмауэра для приложения на Mac	70
Настройка правил брандмауэра для приложения на Mac	71
Удаление правила брандмауэра для приложения на Mac	72
Параметры службы определения расположения на Mac	72
Выключение или включение службы определения расположения на Mac	73
Экспорт параметров блокировки соединения для сетевого расположения	73
Остановка фоновых задач на время игр или при просмотре фильмов на Mac	74
Глава 10 Поиск дополнительных решений	76
Проверка названий и описаний вирусов	76
Поиск ключа или PIN-кода продукта для Mac	77
Проверка типа имеющейся учетной записи пользователя компьютера Mac	78
Удаление Norton на Mac	78

Вас приветствует Norton

В этой главе рассмотрены следующие вопросы:

- [Начало работы с Norton для Mac](#)
- [Требования к системе для Norton Security](#)

Начало работы с Norton для Mac

Norton обеспечивает безопасность компьютера Mac следующими способами.

- Защищает от вирусов, программ-шпионов, вредоносных программ, троянов, фишинга и прочих интернет-угроз.
- Защищает вашу конфиденциальную и финансовую информацию при работе в сети.
- Использует одну из крупнейших глобальных аналитических сетей для более быстрого выявления угроз.

В главном окне Norton для Mac содержатся плитки, нажатие на которые позволяет воспользоваться основными функциями программы:

- **Безопасность**
Убедитесь, что ваше устройство защищено, и исправьте неполадки, если безопасность вашего компьютера находится под угрозой. Большинство видов подписок на Norton позволяют добавить в вашу учетную запись дополнительные устройства, если в ней имеются свободные места.
- **Сканирования**
Выполните быстрое сканирование, полное сканирование или сканирование файлов, чтобы проверить ваше устройство на наличие угроз. Кроме того, вы можете составить график проведения сканирования. Дополнительную информацию см. См. ["Сканирование Norton для проверки Mac на наличие угроз"](#) на стр. 22..
- **LiveUpdate**

Убедитесь, что у вас установлены актуальные средства защиты от угроз, а также расширения для повышения эффективности функций и скорости работы программы. Дополнительную информацию см. См. ["Запуск LiveUpdate для обновления Norton на Mac"](#) на стр. 16..

■ **Дополнительно**

Просматривайте и меняйте параметры работы с компьютером и в сети. Большинству пользователей подходят параметры по умолчанию, однако, при необходимости параметры безопасности и сети можно изменить.

■ **Очистить**

Выполните сканирование системы, чтобы удалить ненужные файлы, которые могут замедлить работу компьютера. Дополнительную информацию см. См. ["Выполните сканирование Norton Clean для удаления файлов, которые снижают скорость работы вашего Mac"](#) на стр. 46..

Требования к системе для Norton Security

Операционная система

Продукт Norton поддерживается только в Mac OS X 10.7.5 (Lion) и более поздних версиях. Если на компьютере установлена система Mac OS X 10.6 или более ранней версии, обновите ее до поддерживаемой версии.

Аппаратное обеспечение

- Компьютер Mac с процессором Intel® Core 2 Duo, Core i3, Core i5, Core i7 или Xeon)
- 2 ГБ оперативной памяти
- 300 МБ свободного дискового пространства
- Подключение к Интернету для LiveUpdate

Поддерживаемые браузеры

- Safari®^{1, 2}
- Mozilla Firefox®^{1, 2}
- Google Chrome™¹

¹ Как предоставляемая компанией Symantec в течение периода обслуживания.

² Поддерживает текущий и последний предыдущий основной 32-разрядный выпуск.

Загрузка и установка продукта Norton

В этой главе рассмотрены следующие вопросы:

- [Загрузка и установка продукта Norton](#)
- [Установка продукта Norton на дополнительных устройствах](#)
- [Перенос лицензии Norton на новое устройство](#)
- [Активация или продление подписки на Norton для Mac](#)

Загрузка и установка продукта Norton

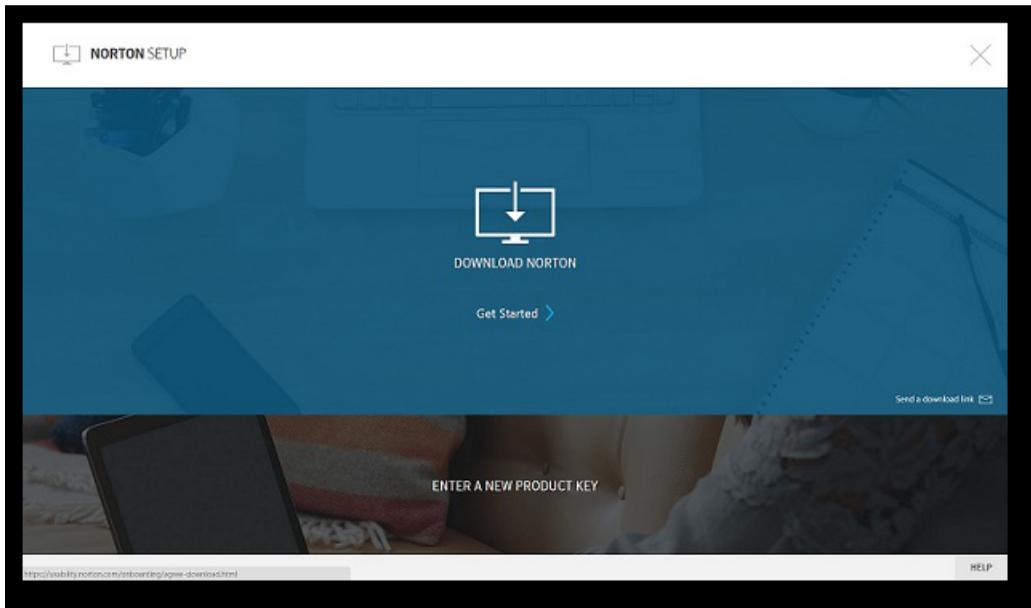
Обеспечивать защиту устройств и управлять продуктом Norton так же просто, как добавить новое устройство к учетной записи Norton.

Как загрузить и установить продукт Norton на компьютере

- 1 Откройте страницу norton.com/setup.
- 2 Если вы не находитесь в учетной записи Norton, нажмите **Войти** и введите адрес вашей электронной почты и пароль от учетной записи Norton.

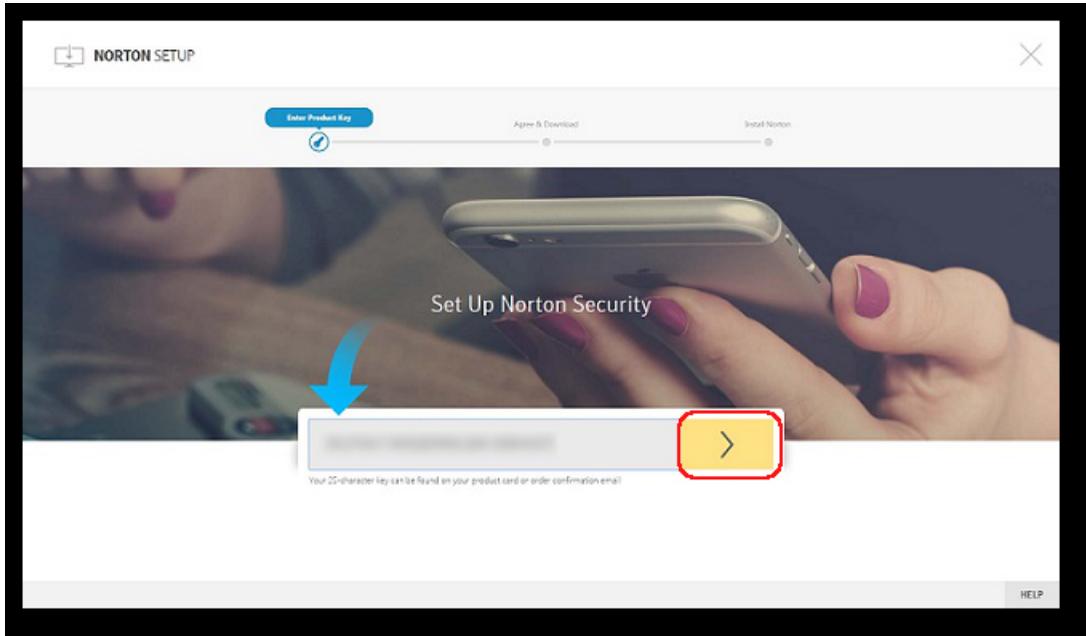
Если у вас нет учетной записи, нажмите **Создать учетную запись** и завершите процесс регистрации.

3 В окне **Настройка Norton** выберите **Загрузить Norton**.



Чтобы установить новый продукт, который еще не зарегистрирован в вашей учетной записи Norton, нажмите **Ввести новый ключ продукта**.

Введите ключ продукта и нажмите значок **Далее (>)**.



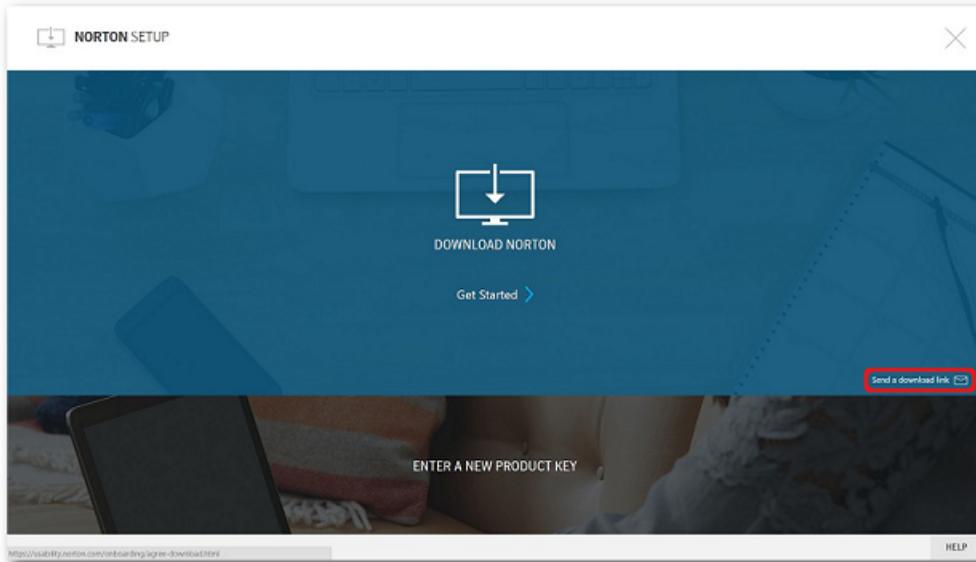
- 4 Нажмите **Принять и загрузить**.
- 5 Нажмите область, на которую указывает синяя стрелка на экране, и следуйте выводимым на экран инструкциям.
 - Для браузера Internet Explorer или Microsoft Edge: нажмите **Выполнить**.
 - В Firefox или Safari: в правом верхнем углу браузера нажмите кнопку **Загрузка**, чтобы открыть список загруженных файлов. Дважды щелкните загруженный файл.
 - В Chrome: в левом нижнем углу браузера нажмите на загруженный файл.
- 6 Если откроется окно **Контроль учетных записей**, нажмите кнопку **Продолжить**.
- 7 Продукт Norton будет загружен, установлен и активирован.

Установка продукта Norton на дополнительных устройствах

Из вашей учетной записи Norton вы можете отправлять электронные письма на дополнительные устройства и устанавливать на них продукты Norton. В электронном письме содержится ссылка для установки продукта Norton и инструкции.

Для установки продукта Norton на другом устройстве

- 1 **Войдите** в учетную запись Norton.
- 2 Если вы не находитесь в учетной записи Norton, нажмите **Войти**, введите адрес вашей электронной почты и пароль от учетной записи Norton и выполните вход.
- 3 В окне **Настройка Norton** выберите **Отправить ссылку для загрузки**.



- 4 Введите адрес электронной почты, к которому можно получить доступ с дополнительного устройства, нажмите кнопку **Отправить**, а затем нажмите **Готово**.
На указанный адрес будет отправлено сообщение электронной почты с инструкциями по установке продукта Norton.
- 5 Откройте сообщение электронной почты, полученное от **коллектива Norton**, на устройстве, на которое вы хотите загрузить продукт Norton.
- 6 Нажмите **Загрузить**.

- 7 Нажмите **Принять и загрузить**.
 - 8 Сохраните файл на компьютере и дважды нажмите его для установки продукта Norton. По умолчанию файл сохраняется в папке Загрузки на компьютерах Mac и Windows.
- Следуйте инструкциям на экране.

Примечание: Продуктом Norton AntiVirus for Mac нельзя управлять с помощью учетной записи Norton.

Перенос лицензии Norton на новое устройство

Если продукт Norton установлен на устройстве, которое больше не используется, вы можете перенести продукт Norton с одного устройства на другое с помощью учетной записи Norton.

Перенос лицензии Norton

- 1 [Войдите](#) в учетную запись Norton.
- 2 На странице **Устройства** определите устройство, для которого больше не требуется защита.

Примечание: Цвет состояния такого устройства должен быть зеленым. Если для устройства, которое больше не используется, отображается состояние красного или оранжевого цвета, вы можете удалить устройство из учетной записи Norton и освободить лицензию.

- 3 Нажмите значок многоточия под устройством.
- 4 В открывшемся меню выберите **Управление лицензиями**.
- 5 На странице **Управление устройством** выполните следующие действия:
 - Нажмите имя устройства.
 - В разделе **Какие действия вы хотите выполнить?** нажмите **Удалить продукт Norton**.
 - Нажмите **Далее**.
- 6 В появившемся окне **Удалить продукт Norton** нажмите **Да**.
- 7 На открывшейся странице нажмите **Установить**.

- 8 На странице **Установить на другом устройстве** выберите один из следующих вариантов:
 - Чтобы установить продукт Norton на текущем устройстве, нажмите **Загрузить**.
 - Для установки продукта Norton на другом устройстве нажмите **Отправить ссылку**.
- 9 Нажмите **Далее**.
- 10 Чтобы завершить установку, следуйте выводимым на экран инструкциям.

Активация или продление подписки на Norton для Mac

Активация продукта — это одна из мер, направленных на защиту от компьютерного пиратства. Кроме того, после активации вы можете быть уверены, что используете оригинальное программное обеспечение Symantec. Активация позволяет получить подписку на продукт Norton на определенный период времени.

Если после установки продукт не был активирован, то, пока это не будет сделано, периодически будет выводиться предупреждение о подписке. Продукт необходимо активировать в течение того периода времени, который указан в предупреждении. В противном случае продукт перестанет работать. Для активации необходимо использовать ключ, прилагаемый к продукту. Для того чтобы продолжить использование продукта Norton, подписку можно продлить.

При подключении к Интернету продукт Norton выдаст запрос на ввод данных учетной записи. Можно воспользоваться имеющейся учетной записью Norton или зарегистрировать новую. После входа в учетную запись Norton можно ввести ключ продукта, чтобы активировать продукт Norton и зарегистрировать ключ продукта в учетной записи Norton. Учетная запись Norton позволяет просматривать сведения, такие как ключ продукта, дата регистрации продукта и последние его обновления.

Активация продукта из предупреждения

- 1 В предупреждении выберите **Активировать**.
- 2 Чтобы активировать продукт, следуйте инструкциям на экране.

Активация продукта из главного окна

- 1 Запустите Norton.
 - Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.
- 2 В главном окне продукта Norton нажмите **Активировать сейчас**.
- 3 В появившемся окне выберите один из следующих вариантов.

- **Активировать сейчас** : следуйте инструкциям на экране. Система предложит ввести ПИН-код продукта, полученный от поставщика услуг.
- **Пропустить** этот параметр позволяет активировать подписку позже.

Описание угроз и реагирование на них

В этой главе рассмотрены следующие вопросы:

- [Исправление, восстановление или удаление файлов, помещенных в карантин](#)
- [Запуск LiveUpdate для обновления Norton на Mac](#)

Исправление, восстановление или удаление файлов, помещенных в карантин

При обнаружении угрозы, которую нельзя устранить с помощью последних описаний вирусов, затронутые файлы помещаются в карантин, чтобы они не распространились по системе и не заразили ваш Mac. Файлы, помещенные в карантин, нельзя использовать или просматривать в **Finder**.

Некоторые приложения могут запрашивать доступ к файлам, помеченным Norton как угрозы и, соответственно, помещенным в карантин. Например, многие условно бесплатные или бесплатные приложения загружают программы показа рекламы, которые делают ваш компьютер уязвимым. Эти приложения не будут работать, если Norton добавит файлы для показа рекламы в карантин.

В окне **Файлы, помещенные в карантин** содержатся дополнительные сведения о файлах, помещенных в карантин. После получения нового описания вируса файл, помещенный в карантин, может быть исправлен. При повторном сканировании угроза может быть удалена из элемента, помещенного в карантин. Такой объект также можно восстановить.

Примечание: Symantec рекомендует не восстанавливать зараженные файлы, если вы не уверены в их безопасности. Если каталог восстановления отличается от исходного размещения, объект может перестать работать. В связи с этим рекомендуется заново установить программу.

В некоторых случаях в Norton отображается уведомление **Файл удален** : это свидетельствует о том, что Norton автоматически обнаружил и переместил зараженный файл в корзину или удалил с вашего Mac файл, который нельзя исправить. Если файл невозможно исправить, он перемещается в карантин или удаляется.

Исправление, восстановление или удаление файла, помещенного в карантин

После загрузки обновлений вируса и их повторной проверки элементы, помещенные в карантин, можно исправить.

- 1 Запустите Norton.
Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.
- 2 В главном окне продукта Norton нажмите **Дополнительно** или **Настройки**.
- 3 На левой панели щелкните **Операции**.
- 4 В строке **Журнал безопасности** щелкните значок просмотра.
- 5 В окне **Журнал безопасности** в разделе **Защитить мой компьютер Mac** щелкните **Поместить в карантин**.
- 6 Выберите объект, который необходимо просмотреть, в списке элементов, помещенных в карантин.
- 7 Щелкните значок «Действия» в левом верхнем углу и выберите одно из следующих действий:
 - **Исправить** : повторное сканирование файла и устранение угрозы.
 - **Восстановить (не рекомендуется)** : перемещение потенциально опасного файла из карантина в его исходное местоположение.
 - **Удалить** : удаление файла из карантина и с вашего Mac.
- 8 Нажмите кнопку **Готово**.

Запуск LiveUpdate для обновления Norton на Mac

По умолчанию Norton загружает и устанавливает самые последние обновления описаний и программ с серверов компании Symantec, чтобы обезопасить ваш компьютер от новых угроз. Если ваш компьютер находился не в сети или вы отключили автоматическое обновление LiveUpdate, можно запустить LiveUpdate в любое время.

Примечание: После установки некоторых обновлений программ может потребоваться перезапустить компьютер.

Запуск LiveUpdate

- 1 Запустите Norton.

Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.

- 2 В главном окне Norton щелкните **LiveUpdate**.
- 3 Нажмите **Просмотреть сводку**, чтобы просмотреть список всех обновлений, загруженных и установленных на компьютере Mac.

Запуск LiveUpdate из окна Мой Norton

- 1 Запустите Norton.
- 2 В главном окне **Мой Norton** в разделе **Безопасность устройства** нажмите **LIVEUPDATE**.
- 3 Нажмите **Просмотреть сводку**, чтобы просмотреть список всех обновлений, загруженных и установленных на компьютере Mac.

Управление безопасностью

В этой главе рассмотрены следующие вопросы:

- [Просмотр и настройка задач, которые Norton выполняет для защиты вашего Mac](#)
- [Просмотр или настройка сетевой активности, которую Norton отслеживает на вашем Mac](#)

Просмотр и настройка задач, которые Norton выполняет для защиты вашего Mac

Norton позволяет просматривать задачи, которые он выполняет для защиты ваших данных, включая запуск сканирования, отправку предупреждений, карантин элементов, блокировку приложений или обнаружение попыток доступа к вашей сети.

Просмотр и настройка задач, которые Norton выполняет для защиты вашего Mac

- 1 Запустите Norton.
Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.
- 2 Нажмите **Дополнительно** или **Настройки** в главном окне продукта Norton.
- 3 На левой панели щелкните **Операции**.
- 4 В строке **Журнал безопасности** щелкните значок просмотра.
- 5 В окне **Журнал безопасности** выберите категорию для просмотра выполненных действий.
- 6 Ознакомьтесь с последней активностью и, при необходимости, выполните следующие действия, доступные для выбранного события:

- Значок



позволяет загрузить отчет в виде текстового файла на диск компьютера Mac.

- Значок



позволяет удалить все записанные события.

- Значок



позволяет фильтровать записанные события на основе ваших требований.

- Значок



позволяет напечатать отчет.

- Значок



позволяет просмотреть дополнительную информацию о выбранном событии.

- Значок



позволяет выполнять доступные для выбранного события действия. Параметры в меню Действие изменяются в зависимости от выбранного в списке события.

- Значок



позволяет настраивать параметры для отображения в каждой категории. В окне **Параметры просмотра журнала безопасности** можно сделать следующие настройки:

- **Показывать имена хоста вместо IP-адресов**
- **Выделять цветом события с высоким уровнем серьезности**
- В раскрывающемся меню **Столбцы** можно выбрать категорию журнала, для которой требуется изменить параметры просмотра. При выборе категории видны типы сведений, которые могут быть отображены. Можно выбрать сведения, которые должны быть показаны в окне Журнал безопасности.

Подробнее

- ◆ ■ См. ["Сканирование Norton для проверки Mac на наличие угроз"](#) на стр. 22.
- См. ["Исправление, восстановление или удаление файлов, помещенных в карантин"](#) на стр. 15.

Просмотр или настройка сетевой активности, которую Norton отслеживает на вашем Mac

Norton позволяет вам просматривать данные об отслеживаемой сетевой активности, включая входящие и исходящие соединения, и приложения, работающие на открытых сетевых портах.

Просмотр или настройка активности сетевых подключений

1 Запустите Norton.

Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.

2 Нажмите **Дополнительно** или **Настройки** в главном окне продукта Norton.

3 На левой панели щелкните **Операции**.

4 В строке **Сетевые операции** щелкните значок просмотра.

5 В окне **Сетевые операции** выберите приложение, службу или порт для просмотра сведений об их текущих сетевых соединениях.

6 Ознакомьтесь с последней активностью сетевых подключений и, при необходимости, выполните следующие действия, доступные для выбранной категории:

- Значок



позволяет загрузить отчет в виде текстового файла на диск компьютера Mac.

- Значок



позволяет напечатать отчет.

- Значок



позволяет просмотреть дополнительную информацию о выбранном событии.

- Значок



позволяет выполнять доступные для выбранного события действия. Параметры в меню Действие изменяются в зависимости от выбранного в списке события.

- Значок



позволяет настраивать параметры для отображения в каждой категории. В окне **Параметры просмотра сетевых операций** можно сделать следующие настройки:

- **Показывать имена хоста вместо IP-адресов**
- В разделе **Столбцы** можно выбрать параметры, которые требуется отображать для соединений.

Подробнее

- ◆ ■ См. "[Начало работы с Norton для Mac](#)" на стр. 6.

Сканирование компьютера Mac

В этой главе рассмотрены следующие вопросы:

- Сканирование Norton для проверки Mac на наличие угроз
- Настройка параметров автоматического сканирования Norton на Mac
- Планирование сканирования Norton на Mac
- Настройка сканирования вашего Mac во время простоя

Сканирование Norton для проверки Mac на наличие угроз

В ходе автоматического сканирования Norton обновляются описания вирусов, а компьютер регулярно проверяется на наличие различных угроз. Если автоматическое сканирование отключено, компьютер был отключен от сети, либо на вашем компьютере мог появиться вирус, вы можете выполнить различные проверки вручную:

- **Быстрое сканирование** : сканирование областей вашего компьютера, которые наиболее уязвимы для угроз.
- **Полное сканирование** : сканирование всей системы, включая менее уязвимые приложения, файлы и выполняемые процессы, которые не проверяются при быстром сканировании.
- **Сканирование файлов** : проверка отдельных файлов или папок, которые могут находиться под угрозой.

Выполнение быстрого сканирования, полного сканирования или сканирования файлов

1 Запустите Norton.

Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.

2 Нажмите **Сканирование** в главном окне Norton.

3 Выберите нужный тип сканирования на левой панели:

- **Быстрое сканирование** > **Запустить быстрое сканирование**
- **Полное сканирование** > **Запустить полное сканирование**
- **Сканирование файлов** > **Выбрать файл**
 Укажите путь к папке или файлу и нажмите **Сканировать**.

Выполнение сканирований из командной строки

Продукт Norton позволяет выполнять различные типы сканирования с помощью интерфейса командной строки. Эта функция, рассчитанная на опытных пользователей, предоставляется компонентом "Сканер Norton" продукта Norton. Эту функцию рекомендуется использовать только опытным пользователям.

Перейдите в раздел **Finder** > **Приложения** > **Утилиты** > **Терминал**, чтобы запустить интерфейс командной строки.

Выполнение быстрого сканирования

- ◆ В командной строке введите `/usr/bin/nortonscanner quickscan`.

Выполнение полного сканирования системы

- ◆ В командной строке введите `/usr/bin/nortonscanner systemscan`.

Сканирование определенного файла

- ◆ В командной строке введите `/usr/bin/nortonscanner -a <file path>`.

Сканирование сжатого файла

- ◆ В командной строке введите `/usr/bin/nortonscanner -c <file path>`.

Сканирование карантина

- ◆ В командной строке введите `/usr/bin/nortonscanner quarantine`.

В окне **Общие сведения о сканировании** представлены общие сведения о последнем выполненном сканировании. При обнаружении зараженных файлов во время сканирования продукт Norton автоматически выполняет соответствующие действия. Сведения о сканировании на вирусы можно просмотреть в окне **Журнал безопасности**.

Примечание: Если продукту Norton не удастся исправить зараженный файл, он помещается в карантин. Таким образом продукт Norton предотвращает заражение других файлов, находящихся на компьютере Mac. Помещенные в карантин элементы представлены в категории Карантин окна Журнал безопасности.

С помощью параметра **Готово** можно закрыть окно Результаты сканирования. Для потенциально нежелательных приложений включена кнопка **Удалить**. С помощью кнопки **Удалить** можно удалить приложение из системы.

Уведомление **Сканирование на наличие вирусов завершено** свидетельствует о том, что зараженные файлы исправлены, и их можно использовать. Сведения об исправленных файлах можно просмотреть с помощью функции **Журнал безопасности** в разделе Операции окна Дополнительно. Также можно просмотреть сведения об обнаруженных вирусах и предпринятых против них действиях по защите компьютера Mac.

Настройка параметров автоматического сканирования Norton на Mac

Автоматическое сканирование Norton максимально повышает безопасность компьютера путем регулярного обновления описаний вирусов, сканирования системы, а также отслеживания входящего и исходящего трафика. Параметры по умолчанию подходят большинству пользователей, однако их можно изменить — например, чтобы проверить конкретные файлы в ходе автоматического сканирования, либо, напротив, проигнорировать их. Кроме того, функцию автоматического сканирования можно временно отключить.

Настройка автоматического сканирования

- 1 Запустите Norton.
 Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.
- 2 Нажмите **Дополнительно** или **Настройки** в главном окне продукта Norton.
- 3 На левой панели щелкните элемент **Защитить мой компьютер Mac**.
- 4 Нажмите значок параметров в строке «Автоматическое сканирование» и установите нужные параметры:
 - **Сканировать все**
 - **Сканировать только эти папки / Не сканировать эти папки**
 Нажмите значок **+** и выберите папки, которые необходимо проверить или проигнорировать в ходе сканирования

- Сканировать файлы, находящиеся в сжатых архивах, включая форматы .zip и .rar.
- Сканировать файлы на внешних дисках при обращении к ним

Планирование сканирования Norton на Mac

После установки Norton на Mac будет включено автоматическое сканирование, при проведении которого обновляются описания вирусов, а система проверяется на наличие различных угроз. Возможно, вы хотите запланировать сканирование на определенное время.

Примечание: Если ваш Mac будет использоваться под другой учетной записью, параметры **Планового сканирования** останутся прежними, а само сканирование будет проводиться в запланированное время.

Планирование сканирования Norton

- 1 Запустите Norton.
Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.
- 2 В главном окне продукта Norton нажмите **Дополнительно** или **Настройки**.
- 3 На левой панели щелкните **Защитить мой компьютер Mac**.
- 4 Убедитесь, что в строке **Плановое сканирование** установлен соответствующий параметр.
Вы не сможете выполнить или настроить плановое сканирование, если параметр отключен.
- 5 Нажмите значок параметров.
- 6 Укажите, какие файлы и папки необходимо проверить, а также установите время проведения сканирования в окне **Плановое сканирование**.
- 7 Нажмите кнопку **Сохранить**.

Настройка сканирования вашего Mac во время простоя

Функция **Сканирование во время простоя** анализирует, используется ли ваш Mac. Если Mac используется, Norton не будет выполнять сканирование, поскольку оно может снизить скорость работы компьютера. Параметры по умолчанию подходят для

большинства пользователей, однако, при необходимости параметры можно изменить так, чтобы сканировать всю систему или только отдельные папки и файлы. Функцию «Сканирование во время простоя» можно отключить (не рекомендуется).

Уведомление **Отчет о сканировании во время простоя** свидетельствует о том, что при сканировании были обнаружены один или несколько зараженных файлов. Для просмотра сведений о зараженных файлах можно использовать параметр **Показать журнал** в окне **Журнал безопасности**

Настройка параметров сканирований во время простоя

1 Запустите Norton.

Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.

2 В главном окне продукта Norton нажмите **Дополнительно** или **Настройки**.

3 На левой панели щелкните **Защитить мой компьютер Mac**.

4 Убедитесь, что в строке **Сканирование во время простоя** установлен соответствующий параметр.

Если переключатель отключен, скорость работы компьютера при его использовании может снизиться.

5 В окне Сканирования во время простоя задайте параметры сканирования:

- **Объекты для сканирования** : сканирование всей системы, загрузочного тома или всех пользовательских папок
- **Сканировать файлы, находящиеся в сжатых архивах (рекомендуется)** : сканирование архивов, например файлов в формате .zip.
- **Просмотр результатов сканирования во время простоя** : сохранение записи результатов сканирования.
- **Восстановить значения по умолчанию** : сброс внесенных изменений и восстановление рекомендованных параметров по умолчанию.

Дополнительная информация

- ◆ ■ См. ["Настройка параметров автоматического сканирования Norton на Mac"](#) на стр. 24.

Обеспечение безопасности в Интернете

В этой главе рассмотрены следующие вопросы:

- Защита от уязвимостей
- Настройте Брандмауэр Norton, чтобы запретить доступ к вашему Mac вредоносным веб-сайтам
- Выключение или включение защиты от уязвимостей
- Исключение или добавление сигнатур атаки на Mac
- Включение или выключение уведомлений о заблокированных сигнатурах атак на Mac
- Параметры брандмауэра для Mac
- Правило брандмауэра для IP-адресов на Mac
- Настройка правил брандмауэра для IP-адреса на Mac
- Изменение правил брандмауэра для IP-адреса на Mac
- Удаление правила брандмауэра для IP-адреса на Mac
- Расширенная защита для Mac
- Выключение или включение компонентов расширенной защиты на Mac
- Настройка загрузки данных из сообщества Norton DeepSight на Mac
- Настройка параметров автоматической блокировки на Mac
- Настройка параметров сигнатур на Mac

- Обновление до последней версии Norton для лучшей защиты вашего Mac
- Помогите Norton Community Watch определить новые потенциальные угрозы для Mac
- Отправка отчетов в Symantec при обнаружении программой Norton ошибки на Mac

Защита от уязвимостей

Функция защиты от уязвимостей помогает обнаруживать и предотвращать вторжения из Интернета. Защита от уязвимостей предоставляет информацию о подверженности программ, установленных на компьютере Mac, атакам вредоносного кода. Она также предоставляет сведения об известных атаках.

Уязвимости представляют собой недоработки в программном обеспечении или операционной системе, ослабляющие общий уровень безопасности компьютера Mac. Причиной появления уязвимостей может быть неправильная настройка компьютера Mac или системы безопасности. Инициаторы внешних атак используют эти уязвимости для выполнения вредоносных действий на компьютере Mac. Примерами атак могут служить мониторинг Active Desktop, перехват ввода с клавиатуры и взлом. Такие атаки могут привести к снижению быстродействия компьютера, сбоям в работе программ и попаданию личных данных и конфиденциальной информации к киберпреступникам.

Продукт Norton обеспечивает защиту компьютера Mac от большинства распространенных атак из Интернета с помощью сигнатур. Сигнатуры атак содержат информацию, сигнализирующую о попытке атакующего воспользоваться известной уязвимостью операционной системы или программ компьютера Mac. Для обнаружения и блокировки подозрительных сетевых операций система предотвращения вторжений продукта Norton применяет обширный список сигнатур атак.

Настройте Брандмауэр Norton, чтобы запретить доступ к вашему Mac вредоносным веб-сайтам

При установке или запуске бесплатного или условно бесплатного ПО некоторые вредоносные веб-сайты попытаются получить несанкционированный доступ к информации на вашем устройстве. Вредоносные веб-сайты обнаруживают и используют уязвимости системы для загрузки вредоносных программ (например, вредоносных программ для майнинга криптовалют), которые раскрывают информацию о вашем устройстве киберпреступникам.

Если параметр **Отслеживание URL-адресов** включен, Norton будет отслеживать все приложения, установленные на вашем устройстве, а также блокировать доступ к вашему устройству вредоносным веб-сайтам. При блокировке вредоносного веб-сайта будет отправлено уведомление. Сведения об атаке можно просмотреть в журнале безопасности.

Примечание: Функция «Отслеживание URL-адресов» не отслеживает приложения браузера. Для защиты приложений браузера от вредоносных веб-сайтов в браузер необходимо добавить расширения Norton. Дополнительную информацию см. См. ["Добавьте расширение Norton в браузер, чтобы повысить безопасность работы и совершения онлайн-покупок на Mac"](#) на стр. 50..

Включение функции «Отслеживание URL-адресов» для блокировки вредоносных веб-сайтов

Функция «Отслеживание URL-адресов» включена по умолчанию. Не выключайте функцию «Отслеживание URL-адресов». В противном случае ваше устройство не будет защищено от атак с вредоносных веб-сайтов.

- 1 Запустите Norton.
Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.
- 2 Нажмите **Дополнительно** или **Настройки** в главном окне продукта Norton.
- 3 Нажмите **Брандмауэр** на левой панели и убедитесь, что переключатель **Защита от уязвимостей** включен.
- 4 В строке **Защита от уязвимостей** щелкните значок параметров.
- 5 Откройте вкладку **Отслеживание URL-адресов** в окне **Защита от уязвимостей**.
- 6 Нажмите **Включить**, если функция отключена.

Исключение URL-адреса или домена из числа отслеживаемых

Для обнаружения и блокировки подозрительных веб-сайтов с помощью функции «Защита от уязвимостей» используется обширный список сигнатур атаки. В некоторых случаях часто используемые веб-сайты могут быть помечены как подозрительные, поскольку они имеют схожие сигнатуры атаки. Если вы уверены, что уведомления о потенциальной атаке вызваны безопасными сайтами или доменами, их можно исключить из числа отслеживаемых.

- 1 Запустите Norton.
Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.
- 2 Нажмите **Дополнительно** или **Настройки** в главном окне продукта Norton.
- 3 Нажмите **Брандмауэр** на левой панели и убедитесь, что переключатель **Защита от уязвимостей** включен.
- 4 В строке **Защита от уязвимостей** щелкните значок параметров.
- 5 Откройте вкладку **Отслеживание URL-адресов** в окне **Защита от уязвимостей**.

- 6 Нажмите кнопку **Добавить** и введите URL-адрес или имя домена, которые необходимо исключить из числа отслеживаемых.
- 7 Нажмите кнопку **Сохранить**.
- 8 Для изменения или удаления URL-адреса или домена необходимо выполнить следующие действия:
 - Выберите URL-адрес или домен из списка и нажмите кнопку **Изменить**. Измените URL-адрес или имя домена и нажмите **Сохранить**.
 - Выберите URL-адрес или домен, который необходимо удалить, и нажмите кнопку **Удалить**.

Просмотр сведений о заблокированном веб-сайте

- 1 Запустите Norton.

Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.
- 2 Нажмите **Дополнительно** или **Настройки** в главном окне продукта Norton.
- 3 На левой панели щелкните **Операции**.
- 4 В строке **Журнал безопасности** щелкните значок просмотра.
- 5 Нажмите **Защита от уязвимостей** в категории **Брандмауэр** в окне **Журнал безопасности**.
- 6 Дважды щелкните сигнатуру атаки левой кнопкой мыши на правой панели, чтобы получить более подробные сведения о заблокированном веб-сайте.
- 7 Нажмите **Подробнее** в окне **Заблокированная уязвимость**, чтобы получить более подробные сведения о сигнатуре атаки.

Выключение или включение защиты от уязвимостей

Можно выбрать, следует ли защищать компьютер Mac от угроз, использующих его уязвимости.

Параметр "Защита от уязвимостей" по умолчанию включен. Symantec рекомендует оставлять включенной защиту от уязвимостей, чтобы защитить компьютер Mac от любых вредоносных атак.

Выключение или включение защиты от уязвимостей

- 1 Запустите Norton.
Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.
- 2 В главном окне продукта Norton выберите **Дополнительно**.
- 3 На левой панели щелкните **Брандмауэр**.
- 4 В строке **Защита от уязвимостей** переместите переключатель в положение Выкл. или Вкл.

Исключение или добавление сигнатур атаки на Mac

Для выявления угроз на компьютере Mac продукт Norton выполняет сканирование, сравнивая сигнатуры файлов с сигнатурами известных атак. Сигнатура атаки используется для выявления попытки инициатора атаки использовать известную уязвимость операционной системы или приложения.

Можно выбрать, следует ли защищать компьютер Mac от всех сигнатур атак или только от отдельных сигнатур. В некоторых случаях повседневные сетевые операции могут оказаться похожими на сигнатуры атак. Возможно получение нескольких уведомлений о возможной атаке. Если вы уверены, что данные уведомления вызваны какой-либо безопасной операцией, то можете исключить сигнатуру этой операции из списка сигнатур атак.

Если необходимо использовать защиту от уязвимостей, но без получения уведомлений о заблокированных атаках, можно выключить отображение соответствующих уведомлений. В отсутствие веских причин для отключения той или иной сигнатуры следует оставить все сигнатуры включенными. Если вы отключите сигнатуру, компьютер может стать уязвимым для атак.

Включение или выключение сигнатур атаки

- 1 Запустите Norton.
Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.
- 2 В главном окне продукта Norton нажмите **Дополнительно** или **Настройки**.
- 3 На левой панели щелкните **Брандмауэр**.
- 4 В строке **Защита от уязвимостей** щелкните значок параметров.
- 5 В окне **Защита от уязвимостей** щелкните вкладку **Сигнатуры**.
- 6 В списке **Сигнатуры** выберите сигнатуру и выполните одно из следующих действий.

- Чтобы отключить обнаружение сигнатур атак, снимите флажок **Включить эту сигнатуру**.
- Чтобы включить обнаружение сигнатур атак, установите флажок **Включить эту сигнатуру**.

7 Щелкните **Готово**.

Включение или выключение уведомлений о заблокированных сигнатурах атак на Mac

Можно выбрать, следует ли защите от уязвимостей показывать уведомления о блокировании потенциальных атак.

Уведомление позволяет выполнять следующие действия.

- Просматривать сведения о заблокированных атаках.
- Отправлять отчеты об ошибочном обнаружении атак.

Все операции функции "Защита от уязвимостей" записываются в окне **Журнал безопасности**. Записи содержат информацию о попытках несанкционированного доступа и другие сведения.

Можно включить или выключить уведомления для всех заблокированных атак или отдельных сигнатур атак.

Включение или выключение уведомлений обо всех заблокированных атаках

1 Запустите Norton.

Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.

2 В главном окне продукта Norton нажмите **Дополнительно** или **Настройки**.

3 На левой панели щелкните **Брандмауэр**.

4 В строке **Защита от уязвимостей** щелкните значок параметров.

5 В окне **Защита от уязвимостей** выберите вкладку **Дополнительно**.

6 На вкладке **Дополнительно** выполните одно из следующих действий.

- Чтобы отключить уведомления о всех заблокированных атаках, отмените выбор параметра **Уведомлять, когда защита от уязвимостей автоматически блокирует атаку**.
- Чтобы включить уведомления о всех заблокированных атаках, выберите параметр **Уведомлять, когда защита от уязвимостей автоматически блокирует атаку**.

7 Щелкните **Готово**.

Включение или выключение уведомлений об отдельных сигнатурах атак

- 1 Запустите Norton.
Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.
- 2 В главном окне продукта Norton нажмите **Дополнительно** или **Настройки**.
- 3 На левой панели щелкните **Брандмауэр**.
- 4 В строке **Защита от уязвимостей** щелкните значок параметров.
- 5 В окне **Защита от уязвимостей** выберите вкладку **Сигнатуры**.
- 6 В списке **Сигнатуры** выполните одно из следующих действий.
 - Чтобы отключить уведомления, отмените выбор параметра **Показать уведомления для этой сигнатуры**.
 - Чтобы включить уведомления, выберите параметр **Показать уведомления для этой сигнатуры**.
- 7 Щелкните **Готово**.

Параметры брандмауэра для Mac

Параметры брандмауэра позволяют настроить порядок мониторинга и реакции брандмауэра на входящие и исходящие сетевые соединения. Параметры брандмауэра включают в себя параметры доступа для приложений, служб и портов компьютера Mac. Также они содержат параметры доступа для входящих и исходящих соединений с другими компьютерами в сети, к которой подключен компьютер Mac.

Окно **Брандмауэр** можно использовать для настройки следующих параметров брандмауэра.

Блокировка приложений

Позволяет настроить правила брандмауэра для соединения с Интернетом приложений, выполняемых на компьютере Mac.

Параметры блокировки приложений определяют, разрешать ли приложению, например веб-браузеру или iTunes, соединение с Интернетом.

Параметры блокировки приложений не связаны с определенным сетевым размещением. Параметры блокировки приложений не изменяются при переходе в другое сетевое размещение.

С помощью параметра **Настроить** в окне **Блокировка приложений** можно настраивать доступ к Интернету для приложений на компьютере Mac.

Примечание: Если параметры блокировки соединения и блокировки приложений перекрываются, более высокий приоритет имеют параметры блокировки соединения.

Блокировка соединения

Позволяет разрешать или блокировать приложения, порты, службы и IP-адреса для выполнения следующих операций.

- Соединение с компьютером Mac.
- Соединение с сетью.

Параметры блокировки соединения определяют, следует ли разрешать или отклонять входящие или исходящие соединения, использующие определенную службу, приложение или порт. Также можно настроить брандмауэр так, чтобы разрешать или блокировать определенный IP-адрес в сети.

Параметры блокировки соединения применяются только для конкретного расположения.

Значок настроек в строке **Блокировка соединения** можно использовать для настройки соединений для приложений и служб на компьютере Mac.

Защита от уязвимостей

Помогает обнаруживать и предотвращать вторжения из Интернета. Функция защиты от уязвимостей отслеживает весь входящий и исходящий трафик компьютера Mac и блокирует любые попытки несанкционированного доступа.

Эта функция предоставляет сведения о подверженности программ, установленных на компьютере Mac, атакам вредоносного кода. Она также предоставляет сведения об известных атаках. Пользователь может контролировать список сигнатур, используемый функцией защиты от уязвимостей.

Служба определения расположения

Позволяет настроить параметры брандмауэра в соответствии с сетевым расположением, к которому подключен компьютер Mac.

Настраиваемые параметры брандмауэра содержат параметры блокировки соединений для приложений и служб, выполняемых на компьютере Mac. При подключении портативного компьютера Mac к новому сетевому расположению продукт Norton предлагает задать параметр брандмауэра для этого сетевого расположения.

DeepSight

Предоставляет доступ к функции "Загрузка данных из сообщества Norton DeepSight", а также ее параметрам. Эта функция позволяет получать актуальный список IP-адресов, идентифицируемых компанией Symantec как атакующие. Функцию загрузки данных из сообщества Norton DeepSight можно включить для получения с серверов Symantec актуального списка IP-адресов.

Правило брандмауэра для IP-адресов на Mac

С помощью окна **Блокировка соединений** можно настроить брандмауэр для зон в сети, к которой подключен компьютер Mac. Можно настроить параметры доступа для зон,

чтобы указать IP-адреса, для которых требуется разрешить или заблокировать соединения.

В **Зоне доверия** на панели **Вид** показаны IP-адреса, попытки доступа к которым или от которых разрешены для сетевого расположения. В **Зоне блокировки** на панели **Вид** показаны IP-адреса, попытки доступа к которым или от которых блокируются для сетевого расположения.

С помощью окна **Блокировка соединений** можно выполнять для зоны следующие операции.

- Настраивать параметры доступа для IP-адреса.
- Изменять параметры доступа для IP-адреса.
- Удалять параметры доступа для IP-адреса.

Настройка правил брандмауэра для IP-адреса на Mac

Можно задать правила брандмауэра для IP-адреса, относящегося к определенному параметру сетевого размещения.

В **Зоне доверия** на панели **Вид** показаны IP-адреса, попытки доступа к которым или от которых разрешены для сетевого расположения. В **Зоне блокировки** на панели **Вид** показаны IP-адреса, попытки доступа к которым или от которых блокируются для сетевого расположения.

Настройка правил брандмауэра для IP-адреса

- 1 Запустите Norton.
Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.
- 2 В главном окне продукта Norton нажмите **Дополнительно** или **Настройки**.
- 3 На левой панели щелкните **Брандмауэр**.
- 4 В строке **Блокировка соединения** щелкните значок параметров.
- 5 В окне **Блокировка соединений** в меню **Изменение параметров** выберите сетевое расположение.
- 6 В меню **Вид** выберите **Зоны**.
- 7 Щелкните **Добавить IP-адрес**.

Также можно указать параметры доступа для IP-адреса с помощью знака **+**, расположенного рядом со строкой **Зона блокировки** или **Зона надежности**.

- 8 В окне **Изменить адрес** выберите параметр доступа по умолчанию. Предусмотрены следующие варианты.

Разрешить	Позволяет разрешить входящие или исходящие соединения со всеми компьютерами, существующими в сети.
Блокировать	Позволяет заблокировать входящие или исходящие соединения с компьютером, имеющим указанный IP-адрес.

- 9 В меню адреса выберите параметр, чтобы указать IP-адреса компьютеров, к которым нужно применить параметры доступа. Предусмотрены следующие варианты.

Все компьютеры в текущей сети	Позволяет разрешить или заблокировать входящие или исходящие соединения со всеми компьютерами в сети.
Один компьютер	Позволяет разрешить или заблокировать входящие или исходящие соединения с компьютером с указанным IP-адресом.
Все IP-адреса, начинающиеся с	Позволяет разрешить или заблокировать входящие или исходящие соединения с компьютерами с указанным базовым адресом.
Все IP-адреса в сети	Позволяет разрешить или заблокировать входящие или исходящие соединения со всеми компьютерами в локальной сети.

- 10 Выберите **Параметры ведения журнала и уведомлений**, чтобы настроить продукт Norton для регистрации попыток доступа и отправки уведомлений о них.

- 11 Нажмите кнопку **Сохранить**.

Изменение правил брандмауэра для IP-адреса на Mac

Можно изменить правило брандмауэра для IP-адреса, относящегося к определенному параметру сетевого расположения.

Изменение правил брандмауэра для IP-адреса

- 1 Запустите Norton.
Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.
- 2 В главном окне продукта Norton нажмите **Дополнительно** или **Настройки**.
- 3 На левой панели щелкните **Брандмауэр**.
- 4 В строке **Блокировка соединения** щелкните значок параметров.
- 5 В меню **Изменение параметров** окна **Блокировка соединений** выберите параметр блокировки соединения, для которого нужно изменить параметры IP-адреса.
- 6 В меню **Вид** щелкните **Зоны** и выберите строку с параметрами доступа для IP-адреса, которые нужно изменить.
- 7 Щелкните пункт **Изменить**.
- 8 В окне **Изменить адрес** внесите нужные изменения.
- 9 Нажмите кнопку **Сохранить**.

Удаление правила брандмауэра для IP-адреса на Mac

Можно удалить правило брандмауэра для IP-адреса определенного сетевого расположения.

Удаление правила брандмауэра для IP-адреса

- 1 Запустите Norton.
Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.
- 2 В главном окне продукта Norton нажмите **Дополнительно** или **Настройки**.
- 3 На левой панели щелкните **Брандмауэр**.
- 4 В строке **Блокировка соединения** щелкните значок параметров.
- 5 В меню **Изменение параметров** окна **Блокировка соединений** выберите параметр блокировки соединений.
- 6 В меню **Вид** выберите **Зоны**.
- 7 На панели **Вид** выберите строку с параметрами доступа IP-адреса и выполните одно из следующих действий:

- Нажмите кнопку **Удалить** и в окне подтверждения еще раз нажмите кнопку **Удалить**.
- Щелкните элемент – рядом с удаляемым IP-адресом и в окне подтверждения еще раз нажмите кнопку **Удалить**.

Расширенная защита для Mac

В окне **Дополнительно** можно настроить дополнительные функции защиты, входящие в состав продукта Norton.

Далее приведен список различных функций расширенной защиты.

Загрузка данных из сообщества Norton DeepSight

Позволяет настроить продукт Norton для автоматического получения актуального списка IP-адресов компьютеров, идентифицируемых Symantec как атакующие.

Защита от уязвимостей

Позволяет настроить продукт Norton для сканирования всего входящего и исходящего сетевого трафика на компьютере Mac и его сравнения с набором *сигнатур атак*.

Сигнатуры атак содержат информацию, которая позволяет выявить попытку атакующего воспользоваться известной уязвимостью операционной системы или программы.

Выключение или включение компонентов расширенной защиты на Mac

В окне **Дополнительно** можно отключать и включать следующие функции расширенной защиты продукта Norton:

- **Загрузка данных из сообщества Norton DeepSight**
- **Защита от уязвимостей**

По умолчанию функции расширенной защиты включены. Рекомендуется не выключать дополнительные функции брандмауэра.

Выключение или включение загрузки данных из сообщества Norton DeepSight

1 Запустите Norton.

Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.

2 В главном окне продукта Norton нажмите **Дополнительно** или **Настройки**.

3 На левой панели щелкните **Брандмауэр**.

4 В строке **DeepSight** щелкните значок параметров.

5 В окне **Параметры Norton DeepSight** откройте вкладку **Загрузки** и выполните одно из следующих действий.

- Чтобы отключить **загрузку данных из сообщества Norton DeepSight**, выберите **Выкл.**
- Чтобы включить **загрузку данных из сообщества Norton DeepSight**, выберите **Вкл.**

6 Щелкните **Готово**.

Выключение или включение защиты от уязвимостей

1 Запустите Norton.

Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.

2 В главном окне продукта Norton нажмите **Дополнительно** или **Настройки**.

3 На левой панели щелкните **Брандмауэр**.

4 В строке **Защита от уязвимостей** переместите переключатель в положение **Выкл.** или **Вкл.**

Настройка загрузки данных из сообщества Norton DeepSight на Mac

Функция **загрузки данных из сообщества Norton DeepSight** позволяет получать актуальный список IP-адресов, идентифицируемых Symantec как атакующие.

Функцию **загрузки данных из сообщества Norton DeepSight** можно включить для получения с серверов Symantec актуального списка IP-адресов.

Функцию **загрузки данных из сообщества Norton DeepSight** можно включить или выключить в окне **Дополнительно** и таким образом разрешить или запретить загрузку информации с серверов Symantec.

Настройка загрузки данных из сообщества Norton DeepSight

- 1 Запустите Norton.

Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.

- 2 В главном окне продукта Norton нажмите **Дополнительно** или **Настройки**.

- 3 На левой панели щелкните **Брандмауэр**.

- 4 В строке **DeepSight** щелкните значок параметров.

В окне **Загрузка данных из сообщества Norton DeepSight** отображается список IP-адресов, идентифицируемых Symantec как атакующие.

- 5 На вкладке **Загрузки** выберите требуемый параметр, чтобы настроить соединения для всех IP-адресов в списке.

Предусмотрены следующие варианты.

Блокировать все соединения

Позволяет заблокировать входящие и исходящие соединения для всех IP-адресов в списке.

Блокировать только входящие соединения

Позволяет блокировать только входящие соединения для IP-адресов в списке.

- 6 Нажмите кнопку **Готово**.

Настройка параметров автоматической блокировки на Mac

Вкладку **Автоматическая блокировка** окна **Защита от уязвимостей** можно использовать для автоматической блокировки IP-адресов компьютеров, которые идентифицированы Symantec как атакующие. При включении параметра **Автоматическая блокировка** продукт Norton добавляет IP-адреса атакующих в список **Адреса, заблокированные функцией автоматической блокировки на данный момент**. С помощью меню **Адреса должны оставаться в списке в течение** можно задать период времени, в течение которого продукту Norton следует блокировать любые соединения с IP-адресом атакующего.

IP-адрес можно удалить из списка **Адреса, заблокированные функцией автоматической блокировки на данный момент** с помощью команды **Удалить**.

Также можно использовать параметр **Исключенные адреса**, чтобы создать исключения для IP-адресов, которые считаются надежными. Продукт Norton разрешает исключенному

адресу устанавливать соединения с системой и не включает этот адрес в список **Адреса, заблокированные функцией автоматической блокировки на данный момент**.

Настройка параметров автоматической блокировки

- 1 Запустите Norton.
Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.
- 2 В главном окне продукта Norton нажмите **Дополнительно** или **Настройки**.
- 3 На левой панели щелкните **Брандмауэр**.
- 4 В строке **Защита от уязвимостей** щелкните значок параметров.
- 5 В окне **Защита от уязвимостей** выберите вкладку **Автоматическая блокировка**.
- 6 Чтобы включить автоматическую блокировку, щелкните параметр **Вкл.**
- 7 Просмотрите список IP-адресов, заблокированных функцией защиты от уязвимостей, в списке **Адреса, заблокированные функцией автоматической блокировки на данный момент**.
- 8 Установите период времени, в течение которого продукт Norton должен блокировать все соединения, в списке **Адреса должны оставаться в списке в течение**.
Значение по умолчанию составляет 30 минут.
- 9 Нажмите кнопку **Готово**.

Настройка параметров сигнатур на Mac

Функция "Защита от уязвимостей" для обнаружения известных атак использует часто обновляемый список сигнатур. Сигнатуры можно просмотреть в списке **Сигнатуры**.

С помощью параметров **Включено** и **Уведомлять** рядом с сигнатурой в списке **Сигнатуры** можно настроить получение предупреждений при попытке доступа, соответствующей какой-либо из сигнатур. По умолчанию все сигнатуры включены и выбраны для уведомления.

Не следует выключать сигнатуры, входящие в список **Сигнатуры**. При выключении какой-либо из сигнатур функция **защиты от уязвимостей** больше не сможет защищать компьютер от соответствующей угрозы.

Можно также включить параметр **Уведомлять, когда защита от уязвимостей автоматически блокирует атаку** для получения предупреждения, как только функция защиты от уязвимостей заблокирует атаку.

Настройка параметров сигнатур

- 1 Запустите Norton.
Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.
- 2 В главном окне продукта Norton нажмите **Дополнительно** или **Настройки**.
- 3 На левой панели щелкните **Брандмауэр**.
- 4 В строке **Защита от уязвимостей** щелкните значок параметров.
- 5 В окне **Защита от уязвимостей** выберите вкладку **Сигнатуры**.
- 6 В списке **Сигнатуры** выключите или включите нужные параметры сигнатур.
- 7 Щелкните **Готово**.

Обновление до последней версии Norton для лучшей защиты вашего Mac

Обновление позволяет загрузить и установить совершенно новую версию защиты устройств Norton и гарантирует, что на вашем Mac установлены самые последние функции обеспечения безопасности. Для работы обновления необходимо находиться в сети.

Примечание: Обновление до последней версии Norton отличается от обновления описаний угроз с помощью LiveUpdate. Обновление можно выполнить только при наличии новой версии защиты устройств Norton. В то же время вы можете в любое время запустить LiveUpdate, чтобы получить последние описания угроз и незначительные улучшения приложения.

Обновление при получении уведомления или предупреждения

Для получения предупреждение или уведомления об обновлениях необходимо включить параметр «Автоматические обновления». Параметр «Автоматические обновления» включен по умолчанию.

- 1 Нажмите **Обновить** в уведомлении об обновлении.
- 2 Если ваша подписка действует:
 - В окне **Бесплатное обновление защиты** нажмите **Обновить**.
 - При запросе пароля учетной записи администратора введите его и нажмите кнопку **Установить помощник**.

- Для завершения процесса обновления нажмите кнопку **Перезапустить**.
- 3 Если срок действия вашей подписки истек:
- Для удаления текущей версии продукта нажмите **Принять и установить**, после чего выберите **Продолжить**.
 - Для удаления нажмите кнопку **Перезапустить**.
 - После перезагрузки компьютера вы сможете выполнить обновление до последней версии Norton или до пробной версии. Прочитайте лицензионное соглашение Norton, а затем нажмите **Принять и установить**.
 - Для завершения процесса обновления нажмите кнопку **Перезапустить**.

Обновление по уведомлению «Обновление доступно» в строке меню Mac

- 1 В строке меню Mac нажмите значок Symantec.
- 2 Нажмите **Доступно обновление**.
- 3 Если ваша подписка действует:
 - В окне **Бесплатное обновление защиты** нажмите **Обновить**.
 - При запросе пароля учетной записи администратора введите его и нажмите кнопку **Установить помощник**.
 - Для завершения процесса обновления нажмите кнопку **Перезапустить**.
- 4 Если срок действия вашей подписки истек:
 - Для удаления текущей версии продукта нажмите **Принять и установить**, после чего выберите **Продолжить**.
 - Для удаления нажмите кнопку **Перезапустить**.
 - После перезагрузки компьютера вы сможете выполнить обновление до последней версии Norton или до пробной версии. Прочитайте лицензионное соглашение Norton, а затем нажмите **Принять и установить**.
 - Для завершения процесса обновления нажмите кнопку **Перезапустить**.

Обновление по уведомлению «Обновление доступно» в раскрывающемся списке «Справка» главного окна Norton

- 1 Запустите Norton.
Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.
- 2 В главном окне продукта Norton нажмите **Справка**.
- 3 Выберите в раскрывающемся меню **Справка** пункт **Доступно обновление**.
- 4 Если ваша подписка действует:

Помогите Norton Community Watch определить новые потенциальные угрозы для Mac

- В окне **Бесплатное обновление защиты** нажмите **Обновить**.
 - При запросе пароля учетной записи администратора введите его и нажмите кнопку **Установить помощник**.
 - Для завершения процесса обновления нажмите кнопку **Перезапустить**.
- 5 Если срок действия вашей подписки истек:
- Для удаления текущей версии продукта нажмите **Принять и установить**, после чего выберите **Продолжить**.
 - Для завершения процесса удаления нажмите кнопку **Перезапустить**.
 - После перезагрузки компьютера вы сможете выполнить обновление до последней версии Norton или до пробной версии. Прочитайте лицензионное соглашение Norton, а затем нажмите **Принять и установить**.
 - Для завершения процесса обновления нажмите кнопку **Перезапустить**.

Выключение или включение автоматических обновлений

- 1 Запустите Norton.
Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.
- 2 Нажмите **Дополнительно** или **Настройки** в главном окне продукта Norton.
- 3 На левой панели нажмите **Параметры продукта**.
- 4 В строке **Автоматические обновления** переместите переключатель в положение **Выкл.** или **Вкл.**

Помогите Norton Community Watch определить новые потенциальные угрозы для Mac

Norton Community Watch позволяет пользователям продуктов Norton улучшить качество идентификации и сократить время на защиту от новых угроз безопасности. Программа собирает определенные данные о безопасности и приложениях, и передает их в Symantec для анализа с целью выявления новых угроз и их источников. Программа помогает создать более качественный и надежный продукт, анализируя данные, отправленные пользователем.

Дополнительные сведения о том, как Norton осуществляет доступ, сбор и обработку данных для определенных продуктов, приведены в [Политике конфиденциальности Norton](#).

Включение и выключение Norton Community Watch

- 1 Запустите Norton.
Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.
- 2 Нажмите **Дополнительно** или **Настройки** в главном окне продукта Norton.
- 3 На левой панели нажмите **Параметры продукта**.
- 4 В строке Norton Community Watch переместите переключатель в положение Выкл. или Вкл.

Отправка отчетов в Symantec при обнаружении программой Norton ошибки на Mac

Служба Norton по управлению ошибками документирует все ошибки, которые возникают при работе продукта Norton. Пользователь всегда может сообщить о ошибках в компанию Symantec.

Включение или выключение компонента Управление обработками ошибок

- 1 Запустите Norton.
Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.
- 2 В главном окне продукта Norton нажмите **Дополнительно** или **Настройки**.
- 3 На левой панели нажмите **Параметры продукта**.
- 4 В строке **Управление обработками ошибок** переместите переключатель в положение Выкл. или Вкл.
- 5 Чтобы разрешить программе Norton отправить подробные данные об ошибке, нажмите значок настроек в окне **Управление ошибками**.
- 6 В окне «Управление ошибками» нажмите **Что собрано?**, чтобы узнать больше о данных, которые собирает Symantec.

Дополнительные сведения о том, как Norton осуществляет доступ, сбор и обработку данных для определенных продуктов, приведены в [Политике конфиденциальности Norton](#).

Поддержание производительности компьютера Mac на высоком уровне

В этой главе рассмотрены следующие вопросы:

- [Выполните сканирование Norton Clean для удаления файлов, которые снижают скорость работы вашего Mac](#)
- [Планирование или настройка сканирования Norton Clean для повышения скорости работы вашего Mac](#)

Выполните сканирование Norton Clean для удаления файлов, которые снижают скорость работы вашего Mac

Ненужные файлы, включая временные файлы, файлы установки, а также дублирующиеся файлы из электронной почты или фотоальбомов могут снизить скорость работы вашего компьютера. Сканирование **Norton Clean** позволяет удалить ненужные файлы различных типов, снижающие скорость работы вашего Mac.

В ходе сканирования **Norton Clean** не проверяются подключенные устройства. Кроме того, выполнение сканирования Norton Clean возможно только на Mac OSX 10.10.5 или более поздней версии. По умолчанию в ходе сканирования Norton Clean ненужные файлы будут перемещены в корзину, но не удалены. Для получения сведений о настройке автоматического удаления ненужных файлов в ходе сканирования Norton Clean см См.

["Планирование или настройка сканирования Norton Clean для повышения скорости работы вашего Mac"](#) на стр. 47.

Выполнение сканирования Norton Clean для удаления ненужных файлов

- 1 Запустите Norton.
Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.
- 2 Нажмите **Clean** в главном окне Norton.
- 3 Затем, нажмите **Выполнить** или **Запустить**.
Если Norton Clean предложит открыть приложения «Фото» и iTunes, нажмите **Открыть**.
- 4 Нажмите **Обзор** в строках «Похожие файлы» и «Дублирующиеся файлы» окна **Просмотр**, выберите файлы, которые необходимо удалить, а затем нажмите **Готово**.
Похожие файлы — файлы, которые кажутся одинаковыми, однако, имеют незначительные отличия (например, различные имена). Дублирующиеся файлы — полностью одинаковые файлы.
- 5 Нажмите **Очистить**, чтобы переместить выбранные файлы в корзину.
В окне **Сканирование Clean завершено** представлены результаты проведенного сканирования.

Планирование или настройка сканирования Norton Clean для повышения скорости работы вашего Mac

Планирование или настройка сканирования Norton Clean

- 1 Запустите Norton.
Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.
- 2 Нажмите **Clean** в главном окне Norton.
- 3 Нажмите значок параметров возле кнопки **Выполнить** или **Запустить** в окне **Clean**.
- 4 Откройте одну из следующих вкладок во всплывающем окне, чтобы запланировать или настроить сканирование:
 - **Общие**
 - Во вкладке **Искать** выберите типы файлов, которые необходимо удалить в ходе сканирования Norton Clean. Для повышения качества сканирования рекомендуется использовать параметры по умолчанию.

- Во вкладке **Планирование сканирования Norton Clean** укажите периодичность проведения сканирования.
- Выберите параметр **Выполнять сканирование Norton Clean** при недостаточном количестве места на диске для автоматического удаления файлов при заполнении дискового пространства.
- Установите флажок для перемещения ненужных файлов в корзину или их безвозвратного удаления при запуске сканирования Norton Clean. Если файлы перемещены в корзину, перед их безвозвратным удалением корзину необходимо очистить.
- **Похожие файлы и повторы**
Параметры по умолчанию подходят для большинства пользователей.
 - Нажмите «Общие» на левой панели и выберите:
Параметры для автоматического открытия приложений **Фото** и **iTunes**, чтобы не получать запросы на их открытие при выполнении сканирования Norton Clean.
Параметр **Выполнить расширенный поиск** для более подробного поиска похожих или дублирующихся файлов в ходе сканирования Norton Clean.
 - Откройте вкладку «Исключения» на левой панели, а затем:
Выберите **Типы файлов**, чтобы добавить или удалить типы файлов, которые необходимо исключить из сканирования.
Нажмите **Расположения**, а затем символ **+**, чтобы указать путь к конкретным файлам и папкам, которые необходимо исключить из сканирования.
 - Откройте вкладку «Типы» на левой панели, а затем:
Измените параметры по умолчанию, выбрав нужные параметры для всех типов файлов.
- **Автовыбор**
 - Нажмите значок **+**.
 - Добавьте правила для файлов, которые необходимо проверить или проигнорировать в ходе сканирования Norton Clean, в раскрывающемся меню окна **Добавить правило автовыбора**.

Защита конфиденциальной информации

В этой главе рассмотрены следующие вопросы:

- [Настройка Norton для обнаружения мошеннических или фишинговых веб-сайтов на Mac](#)
- [Добавьте расширение Norton в браузер, чтобы повысить безопасность работы и совершения онлайн-покупок на Mac](#)

Настройка Norton для обнаружения мошеннических или фишинговых веб-сайтов на Mac

В пакет Norton Device Security входит расширение Safe Web для браузеров Firefox, Safari и Chrome, которое проверяет посещаемые веб-сайты. Расширение автоматически оценивает уровень безопасности веб-сайта и уведомляет вас при обнаружении мошеннических или фишинговых веб-сайтов. Расширение Safe Web защищает вас от киберпреступников, создающих ложные веб-сайты (например, незаконные веб-сайты электронных продаж) для получения вашей финансовой или конфиденциальной информации

Включение и настройка расширения Safe Web

Примечание: Расширение Safe Web доступно только для Mac OS X 10.9 или более ранних версий.

Добавьте расширение Norton в браузер, чтобы повысить безопасность работы и совершения онлайн-покупок на Mac

1 Запустите Norton.

Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.

2 Нажмите **Дополнительно** или **Настройки** в главном окне продукта Norton.

3 Нажмите **Safe Web** на левой панели и убедитесь, что переключатель **Safe Web** включен.

4 Нажмите значок параметров в строке **Safe Web** и установите нужные параметры:

- Улучшить результаты службы поиска для отображения оценок веб-сайтов в результатах поиска.
- Показывать предупреждение при посещении опасного веб-сайта.
- Блокировать опасные веб-сайты.
- Включить функцию защиты от фишинга для оценки уровня безопасности посещаемых веб-сайтов.
- Представлять полный URL-адрес при обнаружении подозрительного веб-сайта для отправки этого адреса Symantec на проверку.

Сделать Norton Safe Search службой поиска по умолчанию

В дополнение к этому можно настроить домашнюю страницу Norton в качестве домашней страницы по умолчанию.

1 Откройте браузер и нажмите значок расширения Safe Web.

2 В появившемся всплывающем окне Safe Web нажмите значок параметров.

3 На странице Параметры браузера выберите параметр Сделать Norton Safe Search службой поиска по умолчанию.

Добавьте расширение Norton в браузер, чтобы повысить безопасность работы и совершения онлайн-покупок на Mac

После установки Norton на Mac, при открытии браузеров Safari, Firefox или Chrome вам будет предложено добавить в них расширения. Norton предоставляет компонент активности браузера, при котором предупреждение о расширении браузера появляется тогда, когда вы активируете браузер. Включите расширения **Norton Safe Web**, **Norton Safe Search**, **Norton Home Page** и **Norton Password Manager**, чтобы максимально повысить уровень безопасности устройств.

Если на вашем устройстве установлена версия Mac OS X 10.10.x или более поздняя, автономные расширения браузера Norton доступны даже после удаления продукта

Добавьте расширение Norton в браузер, чтобы повысить безопасность работы и совершения онлайн-покупок на Mac

Norton. При удалении продукта Norton на версии Mac OS X 10.9 или более ранней все расширения браузера, связанные с Safari и Firefox, будут удалены. Исключение составляют расширения, установленные в браузере Chrome.

Примечание: Автономные расширения **Norton Safe Web**, **Домашняя страница Norton**, **Norton Safe Search** и **Norton Password Manager** не поддерживаются на Mac OS X 10.9 или более ранней версии, а также на более ранних версиях веб-браузеров. Чтобы установить последние расширения браузера Norton, обновите операционную систему Mac и свои веб-браузеры до последних версий.

Добавление расширений браузера для версии Mac OS X 10.10 или более поздней

Safari

Safari 12 и более поздние версии на macOS 10.14.4 (Mojave) и выше

- 1 При первом запуске Safari после установки Norton на экране появится оповещение **Norton Safe Web** или **Norton Safe Web Plus**.
- 2 В окне предупреждения выполните одно из следующих действий:
 - Нажмите **Загрузить**, чтобы установить расширения Norton Safe Web.
 - Нажмите **Напомнить позже**, чтобы отложить установку расширений Norton Safe Web.
 - **Нет, спасибо**. Данный параметр будет доступен после троекратного использования параметра **Напомнить позже**. Вы снова получите предупреждение о расширении браузера, которое будет иметь параметр **Нет, спасибо** вместо **Напомнить позже**. Нажмите параметр **Нет, спасибо**, чтобы игнорировать предупреждение в течение следующих двух недель.

Примечание: Если вашим браузером по умолчанию является Safari, то через две недели вы получите предупреждение **Исправить**. Нажмите **Исправить**, чтобы установить расширения Norton Safe Web. Если предупреждение **Исправить** будет проигнорировано, то предупреждение о расширении браузера Safari появится через 6 месяцев при запуске браузера Safari.

Добавьте расширение Norton в браузер, чтобы повысить безопасность работы и совершения онлайн-покупок на Mac

Подбронные сведения приведены в статье [Расширение Norton Safe Web Plus App for Safari](#).

Firefox

- 1 Когда вы активируете браузер Firefox в первый раз после установки Norton, в новой вкладке автоматически открывается страница Firefox **Защита веб-браузера**. С помощью нее можно установить расширения, включая **Norton Safe Search**, **Домашняя страница Norton**, **Norton Safe Web** и **Norton Password Manager**.

Примечание: Автономное расширение **Norton Safe Search** поддерживается только на последней версии Firefox.

- 2 Используйте параметр **Включить** и следуйте инструкциям на экране для включения расширений браузера. Также можно использовать параметр **Включить все расширения Norton** для установки всех расширений браузера.
- 3 Если для вашего браузера установлено единственное расширение **Norton Password Manager**, то предупреждение о расширении браузера Firefox появится при запуске Firefox спустя одну неделю. В окне предупреждения выполните одно из следующих действий:
 - При нажатии **Добавить** в новой вкладке браузера Firefox автоматически откроется страница **Защита веб-браузера**. Используйте параметр **Включить** и следуйте инструкциям на экране для включения расширений.
 - Нажмите **Напомнить позже**, чтобы отложить установку расширений браузера Norton.
 - **Нет, спасибо**. Данный параметр будет доступен после троекратного использования параметра **Напомнить позже**. Вы снова получите предупреждение о расширении браузера, которое будет иметь параметр **Нет, спасибо** вместо **Напомнить позже**. Нажмите параметр **Нет, спасибо**, чтобы игнорировать предупреждение в течение следующих двух недель.

Примечание: Если вашим браузером по умолчанию является Firefox и для него не установлено разрешение **Norton Safe Web**, то через две недели вы получите предупреждение **Исправить**. Нажмите **Исправить**, чтобы установить расширения браузера. Если предупреждение "Исправить" будет проигнорировано, то предупреждение о расширении браузера Firefox появится через 6 месяцев при запуске браузера Firefox.

Chrome

- 1 Когда вы открываете браузер Chrome в первый раз после установки Norton, в новой вкладке автоматически открывается страница Chrome **Защита веб-браузера**. С помощью нее можно установить расширения, включая **Norton Safe Search**, **Домашняя страница Norton**, **Norton Safe Web** и **Norton Password Manager**.
- 2 Используйте параметр **Нажмите, чтобы добавить** и следуйте инструкциям на экране для включения расширений браузера. Также можно использовать параметр **Добавить все расширения Norton** для установки всех расширений браузера.
- 3 Если для вашего браузера установлено единственное расширение **Norton Password Manager**, то предупреждение о расширении браузера Chrome появится при запуске Chrome спустя одну неделю. В окне предупреждения выполните одно из следующих действий:
 - Нажмите **Добавить**, чтобы автоматически запустить страницу **Защита веб-браузера** в Chrome. Используйте параметр **Нажмите, чтобы добавить** и следуйте инструкциям на экране для включения расширений.
 - Нажмите **Напомнить позже**, чтобы отложить установку расширений браузера Norton.
 - **Нет, спасибо**. Данный параметр будет доступен после троекратного использования параметра **Напомнить позже**. Вы снова получите предупреждение о расширении браузера, которое будет иметь параметр **Нет, спасибо** вместо **Напомнить позже**. Нажмите параметр **Нет, спасибо**, чтобы игнорировать предупреждение в течение следующих двух недель.

Примечание: Если вашим браузером по умолчанию является Chrome и для него не установлено разрешение **Norton Safe Web**, то через две недели вы получите предупреждение **Исправить**. Нажмите **Исправить**, чтобы установить расширения браузера. Если предупреждение "Исправить" будет проигнорировано, то предупреждение о расширении браузера Chrome появится через 6 месяцев при запуске браузера Chrome.

Добавление расширений браузера для версии Mac OS X 10.9 или более ранней

Safari

- 1 Когда вы открываете браузер Safari в первый раз после установки Norton, то продукт Norton отображает предупреждение о расширении браузера, с помощью которого можно установить расширения, включающие доступные для браузеров функции, такие как **Norton Safe Search**, **Домашняя страница Norton** и **Norton Safe Web**.
- 2 Выполните одно из следующих действий:

Добавьте расширение Norton в браузер, чтобы повысить безопасность работы и совершения онлайн-покупок на Mac

- Нажмите **Добавить**, чтобы установить расширение браузера Norton. В новой вкладке браузера Safari автоматически откроется страница "Защита веб-браузера". Используйте параметр "Включить" и следуйте инструкциям на экране для включения этого расширения.
- Нажмите **Напомнить позже**, чтобы отложить установку расширения браузера Norton.
- **Нет, спасибо**. Данный параметр будет доступен после троекратного использования параметра **Напомнить позже**. Вы снова получите предупреждение о расширении браузера, которое будет иметь параметр **Нет, спасибо** вместо **Напомнить позже**. Нажмите параметр **Нет, спасибо**, чтобы игнорировать предупреждение в течение следующих двух недель.

Примечание: Если вашим браузером по умолчанию является Safari и для него не установлено разрешение **Norton Safe Web**, то через две недели вы получите предупреждение **Исправить**. Нажмите **Исправить**, чтобы установить расширения браузера. Если предупреждение "Исправить" будет проигнорировано, то предупреждение о расширении браузера Safari появится через 6 месяцев при запуске браузера Safari.

Firefox

- 1 Когда вы открываете браузер Firefox в первый раз после установки Norton, то продукт Norton отображает предупреждение о расширении браузера, с помощью которого можно установить расширения, включающие доступные для браузеров функции, такие как **Norton Safe Search**, **Домашняя страница Norton** и **Norton Safe Web**.
- 2 Выполните одно из следующих действий:
 - При нажатии **Добавить** в новой вкладке браузера Firefox откроется всплывающее окно расширений. При нажатии **Добавить** в новой вкладке браузера Firefox автоматически откроется страница **Защита веб-браузера**. Используйте параметр **Включить** и следуйте инструкциям на экране для включения расширения.
 - Нажмите **Напомнить позже**, чтобы отложить установку расширения браузера Norton.
 - **Нет, спасибо**. Данный параметр будет доступен после троекратного использования параметра **Напомнить позже**. Вы снова получите предупреждение о расширении браузера, которое будет иметь параметр **Нет, спасибо** вместо **Напомнить позже**. Нажмите параметр **Нет, спасибо**, чтобы игнорировать предупреждение в течение следующих двух недель.

Примечание: Если вашим браузером по умолчанию является Safari и для него не установлено разрешение **Norton Safe Web**, то через две недели вы получите предупреждение **Исправить**. Нажмите **Исправить**, чтобы установить расширения браузера. Если предупреждение "Исправить" будет проигнорировано, то предупреждение о расширении браузера Safari появится через 6 месяцев при запуске браузера Safari.

Chrome

- 1 Когда вы открываете браузер Chrome в первый раз после установки Norton, в новой вкладке автоматически открывается страница Chrome **Защита веб-браузера**. С помощью нее можно установить расширения, включая **Norton Safe Search**, **Домашняя страница Norton** и **Norton Safe Web**.
- 2 Используйте параметр **Нажмите, чтобы добавить** и следуйте инструкциям на экране для включения расширений браузера. Также можно использовать параметр **Добавить все расширения Norton** для установки всех расширений браузера.
- 3 Если вы не установили ни одно из расширений, то предупреждение о расширении браузера Chrome появится при запуске Chrome спустя одну неделю. В окне предупреждения выполните одно из следующих действий:
 - Нажмите **Добавить**, чтобы автоматически запустить страницу **Защита веб-браузера** в Chrome. Используйте параметр **Нажмите, чтобы добавить** и следуйте инструкциям на экране для включения расширений.
 - Нажмите **Напомнить позже**, чтобы отложить установку расширений браузера Norton.
 - **Нет, спасибо**. Данный параметр будет доступен после троекратного использования параметра **Напомнить позже**. Вы снова получите предупреждение о расширении браузера, которое будет иметь параметр **Нет, спасибо** вместо **Напомнить позже**. Нажмите параметр **Нет, спасибо**, чтобы игнорировать предупреждение в течение следующих двух недель.

Примечание: Если вашим браузером по умолчанию является Chrome и для него не установлено разрешение **Norton Safe Web**, то через две недели вы получите предупреждение **Исправить**. Нажмите **Исправить**, чтобы установить расширения браузера. Если предупреждение "Исправить" будет проигнорировано, то предупреждение о расширении браузера Chrome появится через 6 месяцев при запуске браузера Chrome.

Настройка параметров

В этой главе рассмотрены следующие вопросы:

- Параметры блокировки соединения на Mac
- Настройка параметров блокировки соединения на Mac
- Параметры доступа для приложения
- Настройка параметров доступа для приложения
- Параметры доступа для службы
- Настройка параметров доступа для служб
- Настройка особых параметров доступа для службы
- Изменение параметров доступа для службы
- Удаление параметров доступа для службы
- Настройка брандмауэра для приложения на Mac
- Настройка правил брандмауэра для приложения на Mac
- Удаление правила брандмауэра для приложения на Mac
- Параметры службы определения расположения на Mac
- Выключение или включение службы определения расположения на Mac
- Экспорт параметров блокировки соединения для сетевого расположения
- Остановка фоновых задач на время игр или при просмотре фильмов на Mac

Параметры блокировки соединения на Mac

Можно настроить параметры блокировки соединения для приложения, службы или IP-адреса. Исходя из параметров блокировки соединения, брандмауэр разрешает или блокирует входящие и исходящие сетевые соединения.

Настраиваемые параметры блокировки соединения действуют только для выбранного сетевого размещения. Эти параметры применяются только при подключении компьютера Mac к указанному сетевому размещению.

Можно настроить параметры блокировки соединения для следующих элементов.

Приложения	Позволяет задать параметры доступа для приложений, выполняемых на компьютере Mac.
Службы/порты	Позволяет задать параметры доступа для служб и портов, выполняемых на компьютере Mac.
Зоны	Позволяет указать IP-адрес, для которого следует разрешить или заблокировать входящие или исходящие соединения.
Все, в порядке приоритета	<p>Позволяет просмотреть все параметры доступа для выбранного параметра брандмауэра.</p> <p>В случае перекрытия параметров приоритет имеют те из них, которые находятся выше в списке.</p>

Настройка параметров блокировки соединения на Mac

Параметры блокировки соединения применяются к входящим и исходящим соединениям, использующим определенное приложение, службу, порт или IP-адрес.

В окне **Блокировка соединения** можно настроить, разрешается ли приложению или службе подключаться к Интернету или локальной сети. В меню **Изменение параметров** можно выбрать необходимое сетевое расположение и настроить параметры блокировки соединений.

Примечание: Настройка параметров блокировки соединений возможна только при включенном параметре **Блокировка соединения** в окне **Дополнительно**.

Примечание: Для выполнения этой задачи необходима учетная запись пользователя с правами администратора.

Настройка параметров блокировки соединения

- 1 Запустите Norton.
 Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.
- 2 В главном окне продукта Norton нажмите **Дополнительно** или **Настройки**.
- 3 На левой панели щелкните **Брандмауэр**.
- 4 В строке **Блокировка соединения** щелкните значок параметров.
- 5 В окне **Блокировка соединения** откройте меню **Изменение параметров** и выберите сетевое расположение, для которого требуется настроить параметры блокировки соединений.
- 6 Выберите параметр в меню **Вид**.

Набор параметров, отображаемых в меню **Вид**, зависит от сетевого расположения, выбранного в меню **Изменение параметров**.

Предусмотрены следующие варианты.

Приложения	Позволяет задать параметры блокировки соединения для приложений, выполняемых на компьютере Mac.
Службы/порты	Позволяет задать параметры блокировки соединения для служб и портов, выполняемых на компьютере Mac.
Зоны	Позволяет указать IP-адрес, для которого брандмауэр должен разрешить или заблокировать входящие или исходящие соединения.
Все, в порядке приоритета	Позволяет задать текущие параметры блокировки соединения для приложений, служб, портов и зон в порядке приоритета.

7 Выберите одну из следующих вкладок.

Входящий	Позволяет задать параметры доступа для входящих соединений приложения или службы, которая выполняется на компьютере Mac.
Исходящий	Позволяет задать параметры доступа для исходящих соединений приложения или службы, которая выполняется на компьютере Mac.
Входящий и исходящий	Позволяет настроить параметры доступа для входящих и исходящих соединений с указанными IP-адресами. Эта вкладка отображается, только если выбран параметр Зоны в меню Вид .

8 С помощью всплывающего меню **Действие** в нижней части окна **Блокировка соединения** можно указать прочие параметры блокировки соединений. Предусмотрены следующие варианты.

Параметры ведения журнала и уведомлений	Позволяет указать тип попыток доступа, которые должны регистрироваться продуктом Norton. Также можно указать тип попыток доступа, о которых продукт Norton должен уведомлять пользователя.
Дополнительные параметры	Позволяет настроить дополнительные параметры брандмауэра.
Восстановить значения по умолчанию	Позволяет сбросить конфигурацию до настроек по умолчанию.

9 Щелкните **Готово**.

Параметры доступа для приложения

С помощью окна **Блокировка соединений** можно указать параметры доступа для соединения приложений с сетью. Брандмауэр можно настроить так, чтобы он разрешал или блокировал входящие или исходящие сетевые соединения приложений, таких как iTunes.

Также можно настроить параметры доступа по умолчанию и особые параметры доступа для приложения. Параметры доступа по умолчанию применяются для всех входящих и исходящих соединений в сети. Особые параметры доступа позволяют разрешать или блокировать соединения с определенными компьютерами.

С помощью окна **Блокировка соединений** можно выполнять с приложением следующие операции.

- Настраивать параметры доступа.
- Настраивать особые параметры доступа.
- Изменять параметры доступа.
- Удалять параметры доступа.

Настройка параметров доступа для приложения

Продукт Norton позволяет настроить параметры доступа для приложений, выполняемых на компьютере Mac. Исходя из настроенных параметров и сетевого размещения компьютера Mac, брандмауэр разрешает или блокирует входящие и исходящие сетевые соединения.

При настройке параметров доступа для приложения его имя отображается на панели **Вид** окна **Блокировка соединений**. Кроме того, под именем приложения можно увидеть параметр доступа по умолчанию для выбранного приложения.

По умолчанию продукт Norton создает параметр доступа **<Все остальные приложения>**. Этот параметр доступа включает все приложения, выполняемые на компьютере Mac.

Настройка параметров доступа для приложения

1 Запустите Norton.

Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.

2 В главном окне продукта Norton нажмите **Дополнительно** или **Настройки**.

3 На левой панели щелкните **Брандмауэр**.

4 В строке **Блокировка соединения** щелкните значок параметров.

5 В окне **Блокировка соединений** откройте меню **Изменение параметров** и выберите сетевое расположение, для которого нужно настроить параметры доступа.

6 В меню **Вид** выберите **Приложения**.

7 Выберите одну из следующих вкладок.

Входящий	Позволяет задать параметры доступа для входящих соединений приложения.
Исходящий	Позволяет задать параметры доступа для исходящих соединений приложения.

8 Щелкните **Добавить приложение**.

9 В диалоговом окне **Выбор приложения** выберите требуемое приложение.

Если нужное приложение не отображается в списке, щелкните **Прочее**, чтобы найти приложение.

10 В меню, расположенном в верхней части диалогового окна, выберите один из следующих параметров доступа.

Разрешить	Разрешает сетевые соединения для приложения.
Блокировать	Блокирует сетевые соединения для приложения.
Спрашивать	Настраивает брандмауэр для отправки уведомления при попытке программы получить доступ к Интернету.

11 Щелкните пункт **Выбрать**.

Имя добавленного приложения появляется на панели **Вид** окна **Блокировка соединений**.

- 12 С помощью раскрывающегося меню **Действие**, расположенного в нижней части окна **Блокировка соединений**, можно указать расширенные настройки брандмауэра. Предусмотрены следующие варианты.

Параметры ведения журнала и уведомлений	Позволяет указать тип попыток доступа, которые должны регистрироваться продуктом Norton.
Дополнительные параметры	Позволяет настроить дополнительные параметры брандмауэра.
Восстановить значения по умолчанию	Позволяет сбросить конфигурацию до настроек по умолчанию.

- 13 Щелкните **Готово**.

Параметры доступа для службы

В окне **Блокировка соединений** можно настроить параметры доступа для служб, выполняемых на компьютере Mac. Например, можно настроить параметры доступа для службы протокола FTP, которая разрешает доступ к общим папкам на компьютере Mac через порт 21. Можно настроить брандмауэр для протокола FTP, чтобы разрешить или заблокировать входящие и исходящие соединения.

При добавлении существующей службы продукт Norton отображает порт, который эта служба использует для входящих и исходящих соединений.

Также можно задать параметры доступа по умолчанию и особые параметры доступа для службы. Параметры доступа по умолчанию применяются ко всем входящим и исходящим соединениям с компьютерами, использующими службу. Особые параметры доступа позволяют разрешать или блокировать соединения с определенными компьютерами.

С помощью окна **Блокировка соединений** можно выполнять со службой следующие операции.

- Настраивать параметры доступа.
- Настраивать особые параметры доступа.
- Изменять параметры доступа.
- Удалять параметры доступа.

Настройка параметров доступа для служб

Продукт Norton позволяет задать параметры доступа для служб, выполняемых на компьютере Mac. Исходя из заданных параметров доступа и текущего сетевого размещения компьютера Mac, брандмауэр разрешает или блокирует сетевые соединения службы.

Настраиваемые параметры доступа действуют только для выбранного сетевого размещения. Они применяются к компьютеру Mac только при его подключении к сетевому размещению, для которого настроен параметр блокировки соединения.

При добавлении службы ее имя отображается на панели **Вид** окна **Блокировка соединения**. Кроме того, под именем службы можно увидеть параметр доступа по умолчанию для этой службы.

По умолчанию продукт Norton создает параметр доступа **<Все остальные службы>**. Этот параметр доступа включает все службы, выполняемые на компьютере Mac.

Указание параметров доступа для службы

- 1 Запустите Norton.
 Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.
- 2 В главном окне продукта Norton нажмите **Дополнительно** или **Настройки**.
- 3 На левой панели щелкните **Брандмауэр**.
- 4 В строке **Блокировка соединения** щелкните значок параметров.
- 5 В окне **Блокировка соединения** откройте меню **Изменение параметров** и выберите сетевое расположение, для которого нужно настроить параметры доступа.
- 6 В меню **Вид** выберите **Службы/порты**.
- 7 Выберите одну из следующих вкладок.

Входящий	Позволяет задать параметры доступа для входящих соединений службы.
-----------------	--

Исходящий	Позволяет задать параметры доступа для исходящих соединений службы.
------------------	---

- 8 Щелкните **Добавить службу**.

- 9 В открывшемся диалоговом окне **Новая служба** выберите параметр доступа по умолчанию, который нужно применить к службе. Предусмотрены следующие варианты.

Разрешить Разрешает сетевые соединения для службы.

Блокировать Блокирует сетевые соединения для службы.

- 10 Выберите необходимую службу из меню **Имя службы**.

Если служба отсутствует в меню **Имя службы**, введите имя новой службы в меню **Имя службы**. Также можно ввести описание службы в поле **Описание**.

- 11 Вы можете настроить следующие вкладки.

Порты Список портов в брандмауэре, которые служба может открыть.

Параметры **Добавить**, **Изменить** и **Удалить** можно использовать только при добавлении новой службы.

Эти параметры можно использовать для добавления или изменения добавляемых номеров портов.

Ведение журнала Типы соединений, которые продукт Norton должен заносить в журнал.

Уведомления Типы соединений, о которых должен уведомлять продукт Norton при попытке их установить.

Можно выбрать, должен ли брандмауэр разрешать или блокировать попытки соединения службы.

- 12 Нажмите кнопку **Сохранить**.

- 13 С помощью раскрывающегося меню **Действие** в нижней части окна **Блокировка соединения** укажите расширенные настройки брандмауэра. Предусмотрены следующие варианты.

Параметры ведения журнала и уведомлений

Позволяет указать тип попыток доступа, которые должны регистрироваться продуктом Norton.

Также можно указать тип попыток доступа, о которых продукт Norton должен уведомлять пользователя.

Дополнительные параметры

Позволяет настроить дополнительные параметры брандмауэра.

Восстановить значения по умолчанию

Позволяет сбросить конфигурацию до настроек по умолчанию.

- 14 Щелкните **Готово**.

Настройка особых параметров доступа для службы

Продукт Norton позволяет настраивать входящие и исходящие сетевые подключения для каждой службы на компьютере Mac. Можно указать IP-адреса, попытки соединения с которыми следует разрешать или блокировать. Заданные особые параметры доступа отображаются в строке под именем приложения со знаками "минус" (-) и "плюс" (+).

Примечание: Для службы можно добавить любое количество особых параметров доступа. Например, можно добавить для службы особый параметр доступа, разрешающий соединение со всеми компьютерами в сети. Также для той же службы можно добавить другой особый параметр доступа, блокирующий соединение с одним компьютером.

Настройка особых параметров доступа для службы

- 1 Запустите Norton.
 Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.
- 2 В главном окне продукта Norton нажмите **Дополнительно** или **Настройки**.
- 3 На левой панели щелкните **Брандмауэр**.
- 4 В строке **Блокировка соединения** щелкните значок параметров.
- 5 В окне **Блокировка соединений** выберите в меню **Изменение параметров** сетевое расположение, для которого нужно указать особые параметры доступа.

6 В меню **Вид** выберите **Службы/порты**.

7 Выберите одну из следующих вкладок.

Входящий Позволяет задать параметры доступа для входящих соединений службы.

Исходящий Позволяет задать параметры доступа для исходящих соединений службы.

8 На панели **Вид** щелкните знак **+** рядом с именем службы.

9 В диалоговом окне **Изменить адрес** выберите тип доступа для подключений. Предусмотрены следующие варианты.

Разрешить Позволяет разрешить входящие или исходящие соединения с IP-адресом.

Блокировать Позволяет блокировать входящие или исходящие соединения с IP-адресом.

10 Выберите один из следующих вариантов настройки особых параметров доступа.

Все компьютеры в текущей сети Позволяет разрешить или заблокировать входящие или исходящие соединения со всеми компьютерами в сети.

Один компьютер Позволяет разрешить или заблокировать входящие или исходящие соединения с компьютером с указанным IP-адресом.

Все IP-адреса, начинающиеся с Позволяет разрешить или заблокировать входящие или исходящие соединения с компьютерами с указанным базовым адресом.

Все IP-адреса в сети Позволяет разрешить или заблокировать входящие или исходящие соединения со всеми компьютерами в локальной сети.

11 Нажмите кнопку **Сохранить**.

Изменение параметров доступа для службы

Можно изменить следующие параметры доступа для службы:

- Параметры доступа.

- Особые параметры доступа.
- Параметры доступа по умолчанию.

Изменение параметров доступа для службы

1 Запустите Norton.

Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.

2 В главном окне продукта Norton нажмите **Дополнительно** или **Настройки**.

3 На левой панели щелкните **Брандмауэр**.

4 В строке **Блокировка соединения** щелкните значок параметров.

5 В окне **Блокировка соединения** в меню **Изменение параметров** выберите сетевое размещение, для которого требуется изменить параметры блокировки соединений.

6 В меню **Вид** выберите **Службы/порты**.

7 Выберите одну из следующих вкладок.

Входящий	Позволяет задать параметры доступа для входящих соединений службы.
Исходящий	Позволяет задать параметры доступа для исходящих соединений службы.

8 На панели **Вид** выберите строку с именем службы и нажмите кнопку **Изменить**.

9 В диалоговом окне **Изменить службу** внесите необходимые изменения.

10 Нажмите кнопку **Сохранить**.

Изменение особых параметров доступа для службы

1 Запустите Norton.

Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.

2 В главном окне продукта Norton нажмите **Дополнительно** или **Настройки**.

3 На левой панели щелкните **Брандмауэр**.

4 В строке **Блокировка соединения** щелкните значок параметров.

5 В окне **Блокировка соединения** в меню **Изменение параметров** выберите сетевое размещение, для которого требуется изменить параметры блокировки соединений.

6 В меню **Вид** выберите **Службы/порты**.

- 7 На вкладке **Входящие** или **Исходящие** выберите службу, для которой нужно изменить особые параметры доступа.
- 8 На панели **Вид** выберите строку с конкретными параметрами доступа для приложения и нажмите кнопку **Изменить**.
- 9 В окне **Изменить службу** внесите необходимые изменения.
- 10 Нажмите кнопку **Сохранить**.

Изменение параметров доступа по умолчанию для службы

- 1 Запустите Norton.
Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.
- 2 В главном окне продукта Norton нажмите **Дополнительно** или **Настройки**.
- 3 На левой панели щелкните **Брандмауэр**.
- 4 В строке **Блокировка соединения** щелкните значок параметров.
- 5 В окне **Блокировка соединения** в меню **Изменение параметров** выберите сетевое размещение, для которого требуется изменить параметры блокировки соединений.
- 6 В меню **Вид** выберите **Службы/порты**.
- 7 На вкладке **Входящие** или **Исходящие** выберите на панели **Вид** строку с параметрами доступа по умолчанию для службы и нажмите кнопку **Изменить**.
- 8 В открывшемся окне **Действие по умолчанию для <имя службы>** выберите один из следующих параметров.

Разрешить	Разрешает сетевые соединения для службы.
Блокировать	Блокирует сетевые соединения для службы.

- 9 Нажмите кнопку **Сохранить**.

Удаление параметров доступа для службы

Окно **Блокировка соединения** позволяет удалить обычные и особые параметры доступа, настроенные для службы.

Однако отображаемый в списке параметр блокировки соединений по умолчанию удалить нельзя.

Удаление всех параметров доступа для службы

- 1 Запустите Norton.

Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.

- 2 В главном окне продукта Norton нажмите **Дополнительно** или **Настройки**.
- 3 На левой панели щелкните **Брандмауэр**.
- 4 В строке **Блокировка соединения** щелкните значок параметров.
- 5 В окне **Блокировка соединения** в меню **Изменение параметров** выберите сетевое расположение, для которого требуется удалить параметры блокировки соединений.
- 6 В меню **Вид** выберите **Службы/порты**.
- 7 Выберите одну из следующих вкладок.

Входящий

Позволяет задать параметры доступа для входящих соединений службы.

Исходящий

Позволяет задать параметры доступа для исходящих соединений службы.

- 8 Выберите на панели **Вид** нужную службу и выполните одно из следующих действий:
 - Щелкните пункт **Удалить**.
 - Щелкните знак – (минус) рядом с именем службы.
- 9 В окне подтверждения нажмите кнопку **Удалить**.

Удаление отдельного параметра доступа для службы

- 1 Запустите Norton.

Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.

- 2 В главном окне продукта Norton нажмите **Дополнительно** или **Настройки**.
- 3 На левой панели щелкните **Брандмауэр**.
- 4 В строке **Блокировка соединения** щелкните значок параметров.
- 5 В окне **Блокировка соединения** в меню **Изменение параметров** выберите сетевое расположение, для которого требуется удалить параметры блокировки соединений.
- 6 В меню **Вид** выберите **Службы/порты**.

7 Выберите одну из следующих вкладок.

Входящий	Позволяет задать параметры доступа для входящих соединений службы.
Исходящий	Позволяет задать параметры доступа для исходящих соединений службы.

8 На панели **Вид** выберите строку с особыми параметрами доступа для службы и выполните одно из следующих действий:

- Щелкните пункт **Удалить**.
- Щелкните знак – (минус) рядом с именем службы.

9 В окне подтверждения нажмите кнопку **Удалить**.

Настройка брандмауэра для приложения на Mac

Параметры блокировки приложений позволяют настроить правила брандмауэра для различных приложений, выполняемых на компьютере Mac. Исходя из этих параметров, брандмауэр разрешает или блокирует соединения приложения с Интернетом.

Примечание: Параметры брандмауэра для приложений не связаны с сетью, к которой подключен компьютер Mac. Параметры блокировки приложений остаются неизменными независимо от сетевого размещения. Блокировка приложений не позволяет разрешать или блокировать соединения с определенным IP-адресом.

Когда приложение, параметры доступа к Интернету которого не определены, пытается подключиться к Интернету, продукт Norton выводит уведомление. Можно выбрать, следует ли брандмауэру разрешить или блокировать доступ этого приложения к Интернету.

Помимо настройки доступа к Интернету, в окне **Блокировка приложений** для приложения можно выбрать следующие параметры.

Значок поиска	Позволяет найти приложение в списке Параметры .
Добавить приложение	Позволяет добавить приложение и настроить доступ к Интернету вручную.
Удалить	Позволяет удалить выбранное приложение из списка Параметры .

Разрешить приложения, подписанные Apple	Позволяет автоматически разрешать доступ к Интернету приложениям, подписанным Apple.
Уведомлять при попытке использования Интернета заблокированным приложением	Позволяет настроить продукт Norton так, чтобы при любой попытке доступа заблокированного приложения к Интернету отображалось уведомление.
Заносить в журнал все приложения, использующие Интернет	Позволяет регистрировать приложения, осуществляющие доступ к Интернету. Эту информацию можно посмотреть в окне Журнал безопасности .
Восстановить значения по умолчанию	Позволяет сбросить конфигурацию до настроек по умолчанию.

Настройка правил брандмауэра для приложения на Mac

Приложения, выполняемые на компьютере Mac, подключаются к Интернету для загрузки обновлений или для отправки информации о программе. Например, при открытии приложения Apple iTunes оно подключается к Интернету, чтобы получить последнюю информацию для iTunes из магазина приложений. Если вы считаете приложение надежным, вы можете разрешить ему подключаться к Интернету.

В некоторых случаях может понадобиться запретить доступ к Интернету для некоторых приложений. Например, продукт Norton уведомил о попытке приложения подключиться к Интернету. Соединение с Интернетом для приложения можно заблокировать, чтобы предотвратить отправку или получение вредоносной информации данным приложением.

Чтобы настроить доступ приложения к Интернету, можно воспользоваться окном **Блокировка приложений**. Выбранное приложение отобразится в списке **Параметры** окна **Блокировка приложений**. Имя приложения и выбранный параметр брандмауэра отобразятся в списке **Параметры** окна **Блокировка приложений**.

Настройка правил брандмауэра для приложения

- 1 Запустите Norton.

Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.

- 2 В главном окне продукта Norton нажмите **Дополнительно** или **Настройки**.
- 3 На левой панели щелкните **Брандмауэр**.
- 4 В строке **Блокировка приложений** щелкните значок параметров.

- 5 В диалоговом окне **Блокировка приложений** щелкните пункт **Добавить приложение**.
Если нужное приложение не отображается в списке, щелкните пункт **Прочее**, чтобы найти приложение.
- 6 В диалоговом окне **Выбор приложения** выберите требуемое приложение.
- 7 Щелкните пункт **Выбрать**.
Имя добавленного приложения появится в списке **Параметры** окна **Блокировка приложений**.
- 8 Щелкните **Готово**.

Удаление правила брандмауэра для приложения на Mac

Чтобы при необходимости удалить правила брандмауэра, можно воспользоваться окном **Блокировка приложений**.

Примечание: Не удаляйте правила брандмауэра, если у вас нет достаточного опыта работы с программой. Удаление таких правил может повлиять на работу брандмауэра и ослабить защиту компьютера Mac.

Удаление правила брандмауэра для приложения

- 1 В окне **Блокировка приложений** выберите строку с именем приложения.
- 2 Щелкните пункт **Удалить**.
- 3 В окне подтверждения нажмите кнопку **Удалить**.
- 4 Щелкните **Готово**.

Параметры службы определения расположения на Mac

Параметры службы определения размещения позволяют настроить параметры брандмауэра в зависимости от сетевого размещения, к которому подключен компьютер Mac. Настраиваемые параметры брандмауэра содержат параметры блокировки соединений для приложений и служб, выполняемых на компьютере Mac. При подключении портативного компьютера Mac к новому сетевому расположению продукт Norton предлагает задать параметр брандмауэра для этого сетевого расположения.

С помощью окна **Служба определения расположения** можно выполнить следующие действия.

- Включение и выключение службы определения размещения.
- Просмотр текущего сетевого размещения, к которому подключен компьютер Mac.

Выключение или включение службы определения расположения на Mac

Функция **Служба определения расположения** позволяет настроить параметры средства **Блокировка соединений** для каждой сети, к которой подключается компьютер Mac. По умолчанию сеть, к которой компьютер Mac подключен во время установки продукта Norton, относится к категории **Надежные**. При подключении компьютера Mac к сетям с более слабой защитой и более уязвимым сетям такие сети относятся продуктом Norton к категории **Ненадежные**. Но если вы считаете сеть безопасной и надежной, ее категорию можно изменить на **Надежные**.

Функцию **Служба определения расположения** можно включить или отключить в окне **Дополнительно**.

Выключение или включение службы определения расположения

- 1 Запустите Norton.
Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.
- 2 В главном окне продукта Norton нажмите **Дополнительно** или **Настройки**.
- 3 На левой панели щелкните **Брандмауэр**.
- 4 В строке **Служба определения расположения** переместите переключатель в положение **Выкл.** или **Вкл.**

Экспорт параметров блокировки соединения для сетевого расположения

Параметры сетевого расположения можно экспортировать с помощью окна **Экспорт**. Выберите пункт **Экспорт** в меню **Файл** продукта Norton. Продукт Norton экспортирует параметры сетевого расположения в файл NPFX.

Можно использовать следующие варианты экспорта параметров сетевого размещения.

Экспорт всех параметров

Позволяет экспортировать все параметры выбранного сетевого размещения

Экспорт только этих параметров

Позволяет экспортировать только требуемые параметры выбранного сетевого размещения. Доступны следующие параметры.

- Блокировка приложений
- Блокировка соединений
- Приложения
- Службы/порты
- Зоны
- Защита от уязвимостей
- Загрузка данных из сообщества Norton DeepSight™

Защита экспортированных настроек паролем

Позволяет указать пароль для защиты файла экспорта.

Примечание: Для защиты экспортируемых параметров сетевого расположения можно использовать флажок **Защитить паролем экспортируемые параметры**.

Импортировав сохраненные параметры, их можно просмотреть или применить на другом компьютере с установленным продуктом Norton.

Экспорт параметров блокировки соединения для сетевого расположения

- 1 В быстром меню Norton нажмите **Открыть Norton Security**.
- 2 В строке меню продукта Norton выберите **Файл > Экспорт**.
- 3 В окне **Экспорт** выберите требуемый вариант экспорта.
- 4 Нажмите кнопку **Экспорт**.

Остановка фоновых задач на время игр или при просмотре фильмов на Mac

Можно выполнить настройку Norton таким образом, чтобы при выполнении важных задач, просмотре фильмов или запуске игр в полноэкранном режиме приостанавливалось отображение предупреждения и выполнение фоновых задач, снижающих быстродействие компьютера. Для этого просто включите режим без вывода сообщений.

Выключение или включение режима без вывода сообщений

1 Запустите Norton.

Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.

2 Нажмите **Дополнительно** или **Настройки** в главном окне продукта Norton.

3 На левой панели нажмите **Параметры продукта**.

4 В строке **Режим без вывода сообщений** переместите переключатель в положение Выкл. или Вкл.

Поиск дополнительных решений

В этой главе рассмотрены следующие вопросы:

- [Проверка названий и описаний вирусов](#)
- [Поиск ключа или PIN-кода продукта для Mac](#)
- [Проверка типа имеющейся учетной записи пользователя компьютера Mac](#)
- [Удаление Norton на Mac](#)

Проверка названий и описаний вирусов

В окне **Описания вирусов** приведены названия вирусов и соответствующие сведения. Чтобы узнать, защищен ли компьютер Mac от определенного вируса, можно выполнить поиск по названию этого вируса. Norton автоматически обновляет описания вирусов на регулярной основе.

Можно выбрать любой из вирусов и нажать значок **i**, чтобы узнать, насколько серьезно вирус может повлиять на работу компьютера Mac при его заражении. Можно щелкнуть **Дополнительно**, чтобы прочитать сводку. Сводка по каждому вирусу отображается на отдельной веб-странице.

Проверка названий и описаний вирусов

1 Запустите Norton.

Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.

2 Нажмите **Дополнительно** или **Настройки** в главном окне продукта Norton.

3 На левой панели щелкните элемент **Защитить мой компьютер Mac**.

- 4 В строке **Описания вирусов** щелкните значок настроек.
- 5 В окне Описания вирусов введите в поле поиска название или часть названия вируса. Продукт Norton покажет список вирусов с такими названиями. Можно щелкнуть вирус, чтобы узнать о нем подробнее.
- 6 Нажмите кнопку **Готово**.

Дополнительная информация

- ◆ ■ См. "[Настройка параметров автоматического сканирования Norton на Mac](#)" на стр. 24.

Поиск ключа или PIN-кода продукта для Mac

В этой статье приведены сведения о поиске ключа или PIN-кода продукта, необходимых для активации продукта Norton или продления подписки на продукт:

- **Ключ продукта** : строка длиной 25 символов, состоящая из букв и цифр, разделенных дефисами на 5 групп по 5 символов в каждой группе, которая необходима для активации или продления подписки на продукт Norton.

Возможно, поставщик услуг отправил PIN-код на зарегистрированный адрес электронной почты. Если сообщение электронной почты не получено, проверьте папку спама. Если PIN-код так и не удалось найти, обратитесь к поставщику услуг.

- Если продукт установлен на устройство заранее, ключ продукта может храниться в продукте. В этом случае достаточно зарегистрировать продукт в своей учетной записи Norton. После регистрации достаточно будет войти в учетную запись, чтобы узнать ключ продукта. Некоторые производители могут предоставлять ключ продукта на активационной карточке. По всем вопросам следует обращаться к производителям устройства.
- Если продукт Norton был приобретен на стороннем веб-сайте, найдите ключ продукта в сообщении электронной почты с подтверждением заказа. Если сообщения электронной почты нет в папке входящих сообщений, проверьте папку спама.
- Если вы получили карточку с ключом продукта: ключ продукта, а также инструкции по его применению напечатаны на карточке.
- Если карточка Norton приобретена в магазине: ключ продукта напечатан на задней стороне карточки.

Проверка типа имеющейся учетной записи пользователя компьютера Mac

Учетная запись пользователя определяет действия, которые он может выполнять на компьютере Mac. На компьютере Mac можно создать следующие типы учетных записей пользователя:

- учетная запись администратора;
- стандартная учетная запись;
- управляемая учетная запись.

У каждой учетной записи свои права. Учетная запись администратора позволяет получать доступ ко всем областям компьютера Mac, устанавливать и обновлять программное обеспечение, создавать и обслуживать учетные записи других пользователей.

Если вы не знаете, к какому типу относится ваша учетная запись, это можно узнать в **Системных настройках**.

Проверка типа имеющейся учетной записи пользователя компьютера Mac

- 1 В меню **Apple** выберите пункт **Системные настройки**.
- 2 Щелкните элемент **Пользователи и группы**.
- 3 В левой части окна **Пользователи и группы** можно посмотреть имя и тип своей учетной записи.

Удаление Norton на Mac

Чтобы удалить Norton, необходимо знать имя пользователя и пароль учетной записи администратора.

После удаления Norton необходимо перезагрузить компьютер Mac.

Примечание: Для обеспечения постоянной защиты Symantec рекомендует не удалять Norton с компьютера Mac.

Удаление Norton в macOS 10.14.x (Mojave) или более ранней версии

- 1 На панели меню Mac щелкните значок **Norton** и выберите **Открыть Norton**.
- 2 В меню Norton выберите **Norton > Удалить Norton**.
- 3 В появившемся окне нажмите кнопку **Удалить**.
- 4 При запросе введите пароль учетной записи администратора.
- 5 Нажмите **Перезапустить**.

Удалить Norton можно также, перетащив его из папки **Приложения** в **Корзину**.

Удаление Norton в версии macOS 10.15.x (Catalina) или в более поздних версиях

Примечание: Прежде чем следовать приведенным ниже инструкциям, убедитесь, что закрыли приложение Norton.

- 1 Откройте папку **Приложения** на вашем Mac и перетащите значок приложения Norton в **Корзину**.
- 2 Нажмите кнопку **Продолжить**.
- 3 При запросе введите пароль учетной записи администратора и нажмите **ОК**.
- 4 В появившемся окне нажмите кнопку **Удалить**.
- 5 При запросе пароля учетной записи администратора введите его и нажмите кнопку **Установить помощник**.
- 6 Нажмите **Перезапустить**.