

Norton™ AntiVirus Plus

Norton™ 360

Norton™ 360 with LifeLock™

Norton™ 360 for Gamers

Руководство пользователя



Руководство пользователя Norton™ 360 with LifeLock™

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

© NortonLifeLock Inc., 2021 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 NortonLifeLock Inc 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. NORTONLIFELOCK INC. 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 являются "коммерческим программным обеспечением компьютера" в соответствии с определениями, приведенными в FAR 12.212, и попадают под ограничение прав согласно разделам FAR 52.227-19 "Коммерческое программное обеспечение для компьютеров - ограничение прав" и, соответственно, 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 NortonLifeLock 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.

NortonLifeLock Inc.
60 East Rio Salado Parkway,
Suite 1000,
Tempe, AZ 85281

<https://www.nortonlifelock.com>

Оглавление

Глава 1	Вас приветствует Norton LifeLock	6
	Требования к системе для Norton 360	6
	Получение доступа к учетной записи NortonLifeLock	9
Глава 2	Настройка защиты	10
	Настройка безопасности устройства	10
	Настройка Norton Password Manager	11
	Настройка Резервного копирования в облаке	17
	Настройка LifeLock Identity Theft Protection	18
	Отслеживание темной паутины на основе технологии LifeLock**	19
	Настроить защищенную сеть VPN	20
	Настроить средства родительского контроля	21
	Защитите свою банковскую информацию с помощью Norton Safe Web	25
Глава 3	Управление безопасностью устройства	27
	Что делать, если устройство находится под угрозой	27
	Запуск LiveUpdate	28
	Просмотр и исправление угроз безопасности устройства, обнаруженных Norton	29
	Действия при помещении рисков или угроз в карантин	30
	Используйте Norton для оптимизации и повышения производительности компьютера	33
	Запуск сканирования Norton для обнаружения угроз на ПК	37
	Создавайте собственные выборочные сканирования Norton	40
	Планирование сканирования Norton	42
	Просмотр угроз в реальном времени, обнаруженных Norton SONAR	43
	Исключение файлов и папок из сканирований автоматической защиты Norton, SONAR и контроля загрузок	44
	Исключение файлов с сигнатурами низкой степени риска из сканирований Norton	45

Включение и выключение автоматических задач	46
Выполнение пользовательских задач	47
Планирование операций сканирования проблем безопасности и быстрого действия	47
Настройте Защитник данных для блокировки вредоносных процессов, оказывающих угрозу вашему компьютеру	49
Настройка Norton для удаления сценариев, которые могут быть использованы при попытках фишинга	52
Узнайте больше об Управлении сценариями Norton	55
Защитите свое устройство от эксплойтов, хакеров и атак нулевого дня	58
Включение и выключение брандмауэра Norton	60
Настройка правил программы для изменения параметров доступа для программ	60
Изменение порядка обработки правил брандмауэра	61
Временное отключение правила обработки трафика	62
Разрешить доступ к Интернету для заблокированной программы	63
Выключение уведомления о блокировании брандмауэром	64
Подробнее о списке исключений системы предотвращения вторжений	65
Включение защиты веб-браузера	66
Настройка брандмауэра Norton для включения или выключения уведомлений о блокировании атак	67
Включение и выключение функции автоматической блокировки	68
Разблокировка компьютеров, заблокированных функцией автоматической блокировки	68
Добавление устройства в список надежности устройств	69
Включение и выключение контроля загрузок	71
Включение и выключение функции фильтрации спама	71
Ограничение использования Интернета для Norton	72
Включение и выключение функции "Ограничение использования сети"	73
Настройте Norton, чтоб отслеживать приложения и запретить доступ к вашему компьютеру вредоносным веб-сайтам	74
Начало использования резервного копирования в облаке Norton	76
Добавление и исключение файлов и папок из наборов резервного копирования	78

Просмотр и изменение типов и расширений файлов по умолчанию, включаемых Norton в резервное копирование	79
Восстановление изображений, музыки или других важных файлов из наборов данных резервного копирования Norton	80
Удаление набора данных из резервного копирования в облаке	82
Настройка параметров продукта Norton	83
Настройка параметров защиты в реальном времени	84
Подробнее о параметрах Сканирования и угрозы	86
Подробнее о параметрах предотвращения вторжений и защиты браузера	88
Установите параметры Norton таким образом, чтобы вы могли удаленно управлять защищаемыми устройствами	89
Защита параметров безопасности устройства Norton от несанкционированного доступа	90
Установка сочетания клавиш для поиска информации в компоненте «Безопасность устройства Norton»	91
Оптимизация компьютера для игр при помощи Game Optimizer	91
Подробнее о Game Optimizer	93
Как вручную добавить игры в список оптимизированных игр	95
Глава 4 Поиск дополнительных решений	97
Удаление приложения Защита устройства в Windows	97
Заявления об отказе от ответственности	98

Вас приветствует Norton LifeLock

В этой главе рассмотрены следующие вопросы:

- [Требования к системе для Norton 360](#)
- [Получение доступа к учетной записи NortonLifeLock](#)

Требования к системе для Norton 360

Только право на Norton Защита устройства

- Norton™ AntiVirus Plus защищает одно устройство PC или Mac

Права на безопасность устройства и Norton Secure VPN

Поддерживает устройства, работающие на Windows, Mac, Android и iOS

- Norton™ 360 Standard защищает одно устройство
- Norton™ 360 Deluxe защищает до 5 устройств
- Norton™ 360 Premium защищает до 10 устройств
- Norton™ 360 с LifeLock Select защищает до 5 устройств
- Norton™ 360 с LifeLock Advantage защищает до 10 устройств
- Norton™ 360 с LifeLock Ultimate Plus защищает неограниченное количество устройств (действуют ограничения*)
- Norton™ 360 для любителей компьютерных игр защищает до 3 устройств

Примечание: Не все упомянутые выше предложения для защиты NortonLifeLock доступны во всех регионах или для всех партнеров.

Защита устройства

Примечание: Не все функции доступны на всех платформах.

Примечание: Средства родительского контроля, резервное копирование в облаке и SafeCam в настоящее время не поддерживаются в Mac OS.

Операционные системы Windows™

- ◆ ■ Microsoft Windows® 10 (все версии)
 - Microsoft Windows® 10 в режиме S (32-разрядная, 64-разрядная или ARM32) версии 1803 и выше
 - Microsoft Windows® 8/8.1 (все версии)
Некоторые функции защиты недоступны в браузерах начального экрана Windows 8.
 - Microsoft Windows® 7 (32- и 64-разрядная версии) с пакетом обновления 1 или более поздней версии

Примечание: Norton AntiVirus Plus не поддерживается в Windows 10 в режиме S.

Операционные системы Mac®

- ◆ Если у вас продукт Norton 8.0 или более поздней версии, необходимо иметь Mac OS X 10.10.x или более поздних версий.

Примечание: Родительский контроль Norton Family и резервное копирование в облаке в настоящее время не поддерживаются в Mac OS.

Операционные системы Android™

- ◆ Android 6.0 или более поздней версии

Должно быть установлено приложение Google Play.

Автоматическое сканирование приложений в Google Play поддерживается на Android 4.1 или более поздних версиях, за исключением устройств Samsung. Поддерживаются устройства Samsung, работающие на Android 4.2 или более поздних версиях. Для более ранних версий Android необходимо использовать функцию "Поделиться" в Google Play для сканирования приложений.

Операционные системы iOS

- ◆ Смартфоны iPhone и планшеты iPad с текущей и двумя предыдущими версиями Apple iOS

Системные требования Norton™ Secure VPN

Доступно для устройств Windows™ PC, Mac®, iOS и Android™:

Приложение Norton Secure VPN совместимо с PC, Mac, смартфонами и планшетами Android, iPad и iPhone. Вы сможете использовать Norton Secure VPN на указанном количестве устройств в течение срока действия подписки.

Операционные системы Windows™

- ◆ ■ Microsoft Windows® 10 (все версии кроме Windows 10 S)
- Microsoft Windows® 8/8.1 (все версии)
- Microsoft Windows® 7 (32- и 64-разрядная версии) с пакетом обновления 1 или более поздней версии

150 МБ свободного дискового пространства.

Операционные системы Mac®

- ◆ Текущая и две предыдущие версии Mac OS.
- 300 МБ свободного дискового пространства.

Операционные системы Android™

- ◆ Android 6.0 или более поздней версии

Должно быть установлено приложение Google Play.

Операционные системы iOS

- ◆ Смартфоны iPhone и планшеты iPad с текущей и двумя предыдущими версиями Apple iOS

Получение доступа к учетной записи NortonLifeLock

Используя свою учетную запись NortonLifeLock, вы можете управлять сведениями о подписке, найти ключ продукта, активировать автоматическое продление или получить доступ к другим услугам.

Получение доступа к учетной записи

- 1 Перейдите на сайт my.Norton.com и нажмите **Войти**.
- 2 Введите свой адрес электронной почты и имя пользователя и нажмите **Войти**.
- 3 Если вы забыли свой пароль, нажмите **Забыли пароль?** и укажите свой адрес эл. почты.

Если вы увидите сообщение о том, что ваша учетная запись временно заблокирована из-за слишком большого количества неудачных попыток входа, рекомендуется подождать один час и попробовать войти еще раз.

Настройка защиты

В этой главе рассмотрены следующие вопросы:

- [Настройка безопасности устройства](#)
- [Настройка Norton Password Manager](#)
- [Настройка Резервного копирования в облаке](#)
- [Настройка LifeLock Identity Theft Protection](#)
- [Настроить защищенную сеть VPN](#)
- [Настроить средства родительского контроля](#)
- [Защитите свою банковскую информацию с помощью Norton Safe Web](#)

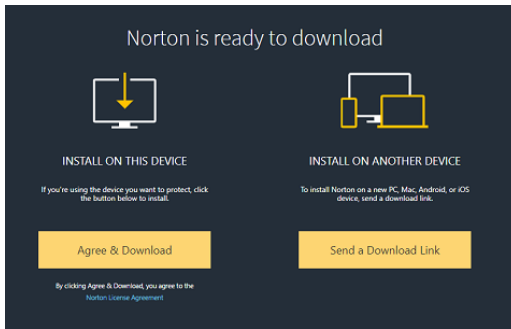
Настройка безопасности устройства

Для защиты вашего устройства необходимо установить Безопасность устройства Norton. Вы можете установить Безопасность устройства на настольные компьютеры и ноутбуки Windows, компьютеры Mac и мобильные устройства, работающие на Android и iOS.

Загрузка и установка продукта Безопасность устройства

- 1 На каждом дополнительном устройстве (настольный компьютер, ноутбук или смартфон) откройте браузер и введите следующий URL:
<https://norton.com/setup>
- 2 Войдите в учетную запись NortonLifeLock.

- 3 В окне **Настройка Norton** нажмите кнопку **Принять и загрузить**.



- 4 Щелкните область, на которую указывает стрелка на экране, и следуйте выводимым на экран инструкциям.

Услуга будет загружена, установлена и активирована автоматически.

Примечание: Если загрузка не была завершена или в процессе загрузки услуги произошла ошибка, загрузку можно перезапустить.

Настройка Norton Password Manager

После установки приложения Безопасность устройства вам будет предложено добавить расширения браузера. Чтобы обеспечить работу компонентов, необходимо добавить расширения в браузеры Internet Explorer, Firefox и Chrome.

Включите расширения браузеров Norton, чтобы получить доступ ко всем функциям, доступным для браузеров. Расширения браузера Norton включают в себя:

Norton Safe Web

Безопасный поиск, который повышает безопасность при просмотре веб-страниц, поиске и совершении покупок в Интернете. Эта функция анализирует посещаемые веб-сайты и определяет наличие на них вирусов, программ-шпионов, вредоносных программ и других угроз безопасности.

Norton Safe Search

Защищенная служба поиска, использующая ресурсы Ask.com и Yahoo! для получения результатов поиска в Интернете. Norton Safe Search ранжирует результаты поиска на основе сведений о безопасности сайтов и рейтинга Norton.

Домашняя страница Norton

Веб-сайт, на котором используется Norton Safe Search для расширения возможностей поиска в Интернете. Пользователю предоставляется информация о состоянии безопасности веб-сайта и рейтинге Norton для каждого результата поиска.

Norton Password Manager

Безопасное расположение, в котором можно хранить все конфиденциальные сведения, например учетные данные, личную и финансовую информацию. Эти сведения можно использовать для входа на веб-сайты, автоматического заполнения интерактивных форм и платежей в Интернете.

Internet Explorer

Добавление расширений браузера Norton в Internet Explorer

- 1 После первой установки продукта Norton при запуске нового сеанса Internet Explorer автоматически откроется страница **Защита веб-браузера** в новой вкладке или новом окне.
- 2 На странице **Защита веб-браузера** выберите значение **Включить** для параметра **Панель инструментов Norton Security**.
- 3 Во всплывающем окне расширений нажмите **Добавить расширение**.
- 4 После включения панели инструментов Norton Security можно включить в браузере расширения Norton Safe Search, Домашняя страница Norton и Norton Password Manager.
Используйте параметр **Нажмите, чтобы добавить** и следуйте инструкциям на экране для включения этих функций.
- 5 Если ни одно из этих расширений не установлено, по прошествии недели в Internet Explorer отобразится **предупреждение о защите Internet Explorer**.
Нажмите **Установить** и следуйте инструкциям на экране, чтобы установить расширения.

Примечание: Чтобы включить расширение Norton позже, нажмите **Напомнить позже**. Если необходимо отключить уведомление, нажмите **Больше не спрашивать**.

Google Chrome

Добавление расширений браузера Norton в Google Chrome

Примечание: Для установки расширений браузера Google Chrome необходима последняя версия Norton 360. Если последняя версия не установлена на вашем компьютере, запустите LiveUpdate в продукте Norton. Мы предлагаем следующие расширения для браузера Google Chrome:

- Norton Safe Web
 - Norton Password Manager
 - Norton Safe Search
 - Домашняя страница Norton
 Установите расширения браузера для Chrome, следуя приведенным ниже инструкциям.
- 1 После первой установки продукта Безопасность устройства при запуске нового сеанса Google Chrome автоматически откроется страница **Защита веб-браузера** в новой вкладке или новом окне.

 Страницу **Защита веб-браузера** также можно открыть, нажав **Настроить** на панели **Безопасность в Интернете**.
 - 2 На странице **Защита веб-браузера** выберите **Нажмите, чтобы добавить** в окне **Norton Safe Web**.
 - 3 Во всплывающем окне расширений нажмите **Добавить расширение**.
 - 4 После включения Norton Safe Web можно включить в браузере компоненты Norton Safe Search, Домашняя страница Norton и Norton Password Manager. Используйте кнопку **Нажмите, чтобы добавить** и следуйте инструкциям на экране для включения этих расширений.

 Для включения всех расширений Norton в Google Chrome нажмите **Добавить все расширения Norton бесплатно** и следуйте инструкциям на экране.
- Если расширение Norton Safe Web не установлено, по прошествии недели при запуске Google Chrome отобразится предупреждение **Защита Chrome удалена**.

- Если ни одно из этих расширений не установлено, по прошествии недели в Google Chrome отобразится **предупреждение о защите Google Chrome**.
- 5 Нажмите **Установить** и следуйте инструкциям на экране, чтобы установить расширения.

Примечание: Чтобы включить расширение Norton позже, нажмите **Напомнить позже**. Если необходимо отключить напоминания, нажмите **Больше не спрашивать**.

Mozilla Firefox

Добавление компонентов браузера Norton в Mozilla Firefox

Примечание: Для установки автономных расширений браузера Mozilla Firefox необходима последняя версия Norton 360. Если последняя версия не установлена на вашем компьютере, запустите LiveUpdate в продукте Norton. Мы предлагаем следующие расширения для браузера Firefox:

- Norton Safe Web
 - Norton Safe Search
 - Домашняя страница Norton
 - Norton Password Manager
- Установите и обновите расширения браузера для Firefox, следуя инструкциям, приведенным ниже.

- 1 После первой установки продукта Безопасность устройства при запуске нового сеанса Mozilla Firefox автоматически откроется страница **Защита веб-браузера** в новой вкладке или новом окне.

Если продукт Norton Безопасность устройства был обновлен, нажмите **ОК** в окне предупреждения **Защита веб-браузера** для отображения страницы расширений.

Примечание: Страницу **Защита веб-браузера** также можно открыть, нажав **Настроить** на панели **Безопасность в Интернете**.

- 2 На странице **Защита веб-браузера** выберите параметр **Включить** для **Norton Safe Web**.

- 3 Во всплывающем окне расширений нажмите **Разрешить**.

После включения Norton Safe Web можно включить в браузере компоненты Norton Safe Search, Домашняя страница Norton и Norton Password Manager. Используйте параметр **Включить** и следуйте инструкциям на экране для включения этих компонентов.

Для включения всех расширений Norton в Firefox нажмите **Добавить все расширения Norton бесплатно** и следуйте инструкциям на экране.

Если расширения не установлены, по прошествии недели в Mozilla Firefox при запуске отобразится **Предупреждение Firefox о защите**. Чтобы включить расширение Norton позже, нажмите **Напомнить позже**. Если необходимо отключить напоминания, нажмите **Больше не спрашивать**. При выборе параметра **Напомнить позже** по прошествии недели в браузере Firefox отобразится предупреждение о защите. Нажмите параметр **Установить** в уведомлении и следуйте инструкциям на экране, чтобы установить разрешения.

Microsoft Edge

Добавление расширения браузера Norton в Microsoft Edge

Примечание: Norton Password Manager — это автономное расширение, для которого не требуется установка продукта Norton в браузере Microsoft Edge. Это расширение совместимо только с компьютерами под управлением Windows 10 Creators Update и более поздних версий.

- 1 Запустите браузер Microsoft Edge.
- 2 Нажмите кнопку **Дополнительно** в правом верхнем углу и выберите пункт **Расширения**.
- 3 В окне **Расширения** нажмите **Получить расширения из магазина**.

- 4 В окне **Магазин** введите в строке поиска **Norton** и выберите **Norton Password Manager** в результатах поиска.
- 5 Нажмите кнопку **Установить**.
 После установки расширения нажмите кнопку **Запуск**.
- 6 В окне **Новое всплывающее окно расширения** нажмите **Включить**.
- 7 Чтобы отобразить значок Norton Password Manager в адресной строке, нажмите кнопку **Дополнительно** в верхнем правом углу браузера и выберите **Расширения**.
- 8 В окне **Расширения** выберите **Norton Password Manager**.
- 9 В окне **Norton Password Manager** перейдите к строке **Показывать кнопку рядом с адресной строкой** и переместите ползунок в положение **Вкл**.

Расширения браузера для Microsoft Edge на основе Chromium

Microsoft выпустила новую версию Microsoft Edge на основе проекта с открытым кодом Chromium. Norton предлагает следующие расширения браузера для новой версии браузера в магазине Microsoft Edge.

- Norton Password Manager предоставляет инструменты, необходимые для создания, хранения и управления вашими паролями, информацией о кредитной карте и другой конфиденциальной информацией в Интернете — для улучшенной защиты
- Norton Safe Web обеспечивает защиту от угроз из Интернета во время просмотра веб-страниц.

Расширения доступны для платформ Windows и Mac.

Добавление расширения Norton Safe Web в Microsoft Edge

- 1 Запустите браузер Microsoft Edge.
- 2 Запустите [расширение Norton Safe Web](#) со страницы настроек Microsoft Edge.

Примечание: Вы можете щелкнуть значок параметров > **Расширения**, чтобы проверите, установлено ли расширение Norton Password Manager. На странице **Расширения** переместите ползунок Norton Safe Web, чтобы включить это расширение.

- 3 На странице настроек Norton Safe Web нажмите **Получить**.
- 4 Нажмите **Добавить расширение** во всплывающем окне **Добавить "Norton Safe Web" в Microsoft Edge**, чтобы установить расширение Norton Safe Web.

Добавление расширения Norton Password Manager в Microsoft Edge

- 1 Запустите браузер Microsoft Edge.
- 2 Запустите [расширение Norton Password Manager](#) со страницы надстроек Microsoft Edge.

Примечание: Вы можете щелкнуть значок параметров > **Расширения**, чтобы проверить, установлено ли расширение Norton Password Manager. На странице **Расширения** переместите ползунок Norton Password Manager, чтобы включить это расширение.

- 3 На странице надстроек Norton Password Manager нажмите **Получить**.
- 4 Нажмите **Добавить расширение** во всплывающем окне **Добавить "Norton Password Manager" в Microsoft Edge**, чтобы установить расширение Norton Password Manager.

Настройка Резервного копирования в облаке

Резервное копирование в облаке служит профилактической мерой на случай неустранимого сбоя компьютера или потери данных из-за его заражения программой-вымогателем или вредоносной программой. Ваша подписка дает право на определенный объем пространства для резервного копирования в облаке Norton. Этот объем зависит от приобретенной вами подписки.

Примечание: Компонент резервного копирования в облаке Norton доступен только в Windows.

Перед запуском первой резервной копии необходимо активировать резервное копирование в облаке.

Примечание: Для использования резервного копирования в облаке необходимо установить для параметра **Ограничение использования сети** в окне **Параметры брандмауэра** значение **Без ограничений**.

Активация Резервного копирования в облаке

- 1 Запустите Norton.
- 2 В окне **Мой Norton**, рядом с пунктом **Резервное копирование в облаке** нажмите **Настроить**.
- 3 В появившемся окне нажмите кнопку **Активировать резервное копирование**.

- 4 При появлении запроса на вход введите адрес эл. почты и пароль учетной записи NortonLifeLock и нажмите **Вход**.
- 5 Нажмите **Готово**.

Настройка LifeLock Identity Theft Protection

Объединив усилия компаний LifeLock и Norton, мы помогаем защитить ваши идентификационные данные.

Вы можете добавить следующую личную информацию для отслеживания† в LifeLock:

- Водительские права
- Номер социального страхования, дата рождения, девичья фамилия матери
- 5 страховых удостоверений
- 5 адресов
- 5 номеров телефона
- 10 банковских счетов
- 10 кредитных карт*

Вы можете добавить дополнительную информацию для отслеживания LifeLock, например, дополнительные номера телефонов, адреса электронной почты или учетные записи.

Система оповещения LifeLock предупреждает вас†, когда кто-то использует ваши идентификационные данные. Это может быть попытка получить автокредит на ваше имя или доступ к учетной записи мобильного телефона.

Примечание: LifeLock Identity Theft Protection не распространяется на коммерческие организации. Наши технологии и услуги предназначены для защиты лиц, имеющих информацию, позволяющую установить личность, такую как номера социального страхования, которой нет у компаний.

*Могут быть добавлены основные кредитные карты, такие как Visa, MasterCard, American Express и Discover. К сожалению, в настоящее время другие типы карт, такие как карты розничных магазинов или подарочные карты, не поддерживаются.

Невозможно предотвратить все кражи идентификационных данных или киберпреступления.

†LifeLock не контролирует все транзакции всех компаний.

Настройка LifeLock Identity Theft Protection

- 1 Запустите Norton.
- 2 В окне **Мой Norton**, рядом с пунктом **Защита идентификационных данных** нажмите **Настроить**.
- 3 На странице **Вход для пользователей LifeLock** нажмите **Вход с помощью Norton**.
- 4 Введите идентификационные данные учетной записи и войдите в систему.
- 5 Следуйте инструкциям на экране.

Установка приложение LifeLock для Norton 360 на Android

- 1 На устройстве Android запустите приложение **Play Store** и выполните поиск **LifeLock Identity Theft Protection**.
- 2 На странице приложения в Play Store нажмите **Установить**, а затем **Принять**.
- 3 После установки приложения войдите в него, используя данные своей учетной записи.

Установка приложение LifeLock для Norton 360 на iOS

- 1 На устройстве iOS запустите приложение **App Store** и выполните поиск **LifeLock Identity Theft Protection**.
- 2 На странице приложения в App Store нажмите **Получить**, а затем **Установить**.
- 3 После установки приложения войдите в него, используя данные своей учетной записи.

Отслеживание темной паутины на основе технологии LifeLock**

Что такое отслеживание темной паутины?

Мы следим за использованием вашей личной информации** на труднонаходимых теневых веб-сайтах и форумах. Мы уведомим вас при обнаружении ваших данных в темной паутине.

Почему это так важно?

Злоумышленники, крадущие идентификационные данные, могут продавать их на труднонаходимых теневых веб-сайтах и форумах.

Что вам необходимо сделать?

Если вы обнаружите свои данные в уведомлении, выполните указанные ниже действия.

- **Угроза безопасности дебетовой/кредитной карты** : если карта закрыта, никаких действий предпринимать не нужно. Если счет открыт, обратитесь в компанию,

выдавшую кредитную/дебетовую карту, и сделайте запрос на новую карту. Внимательно следите за состоянием вашего счета.

- **Угроза безопасности электронной почты** : измените текущий пароль электронной почты. Если у вас есть учетные записи с тем же паролем, также измените и их. Если у вас есть проблемы с электронной почтой, вы можете открыть новую учетную запись электронной почты. Помните, что смена паролей каждые 30 дней поможет обеспечить безопасность ваших учетных записей.
- **Угроза безопасности номера социального страхования** : рекомендуем разместить предупреждения о мошенничестве в одном из трех бюро кредитных историй, чтобы дополнительно защитить ваши идентификационные данные.
- **Угроза безопасности имени/адреса/номера телефона** : к счастью, в этом случае не передается потенциально более опасная информация, например, ваш номер социального страхования. Однако, поскольку некоторые ваши личные данные можно увидеть, мы рекомендуем внимательно следить за кредитным отчетом на предмет возможных несоответствий.

Мы продолжим отслеживать наличие вашей личной информации** в "темной паутине". При обнаружении ваших данных вам будет выслано еще одно электронное письмо.

Примечание: Невозможно предотвратить все кражи идентификационных данных.

**Отслеживание темной паутины в планах Norton 360 по умолчанию относится только к вашему адресу электронной почты. Войдите на портал, чтобы проверить, можете ли вы добавить дополнительную информацию для отслеживания.

Настроить защищенную сеть VPN

Общедоступные сети Wi-Fi есть повсюду: в аэропортах, кафе, торговых центрах и отелях. Бесплатных хот-спотов так много, что люди подключаются к сети, не задумываясь лишней раз. Однако чтение электронной почты, проверка банковского счета или выполнение каких-либо действий, требующих входа в систему, может представлять опасность при использовании общедоступных сетей Wi-Fi. При использовании общедоступных сетей Wi-Fi ваши действия могут отслеживаться. Киберпреступники могут похитить личную информацию: имена пользователей, пароли, расположение, чаты, сообщения электронной почты или номера банковских счетов.

Secure VPN помогает защитить ваше соединение при использовании общедоступного беспроводного соединения. Оно создает виртуальную частную сеть (VPN), которая зашифровывает конфиденциальные данные.

Secure VPN защищает отправляемые и получаемые данные в общедоступных сетях Wi-Fi следующими способами:

- Добавляет шифрование банковского уровня для защиты соединения в общедоступных хот-спотах Wi-Fi.
- Позволяет анонимно просматривать веб-страницы для сохранения вашей конфиденциальности в Интернете.
- Позволяет получать доступ к вашим любимым приложениям и ресурсам в любом месте, как если бы вы подключались к сети из дома.
- Шифрует ваши данные с помощью виртуальной частной сети, которая не отслеживает и не сохраняет ваши действия.
- Предлагает высококлассную поддержку для пользователей продуктов Norton LifeLock, лидера в области сетевой безопасности.

Примечание: Компонент Secure VPN доступен не для всех подписок.

Следуйте приведенным ниже инструкциям, чтобы настроить защищенную сеть VPN.

Настройка Secure VPN

- 1 Запустите Norton.
- 2 В окне **Мой Norton**, рядом с пунктом **Защищенная сеть VPN**, нажмите **Настроить**.
- 3 На открывшейся веб-странице нажмите **Вход в систему**.
- 4 Введите идентификационные данные учетной записи и войдите в систему.
- 5 Если выводится предложение на загрузку, нажмите **Загрузить**.
- 6 Следуйте инструкциям, выводимым на экран.

Присоединяйтесь к обсуждению с другими пользователями настольных компьютеров по ссылке [Norton Community](#).

Настроить средства родительского контроля

Теперь вы можете настроить родительский контроль, чтобы обеспечить безопасность детей в Интернете. Это можно сделать за три простых шага.

Средства родительского контроля предоставляют все необходимое для защиты семьи от угроз и нежелательного содержимого в Интернете. В дополнение к этому, они помогают уберечь ребенка от разглашения конфиденциальной информации в сети.

Вход в учетную запись NortonLifeLock

- 1 Запустите Norton.
- 2 В окне **Мой Norton**, рядом с пунктом **Средства родительского контроля** нажмите **Настроить**.

- 3 Если вам будет предложено войти в систему, введите данные учетной записи и выполните вход.
- 4 На открывшейся странице нажмите вкладку **Семья**.
- 5 Прочитайте **Условия предоставления услуг** и нажмите **Принять и продолжить** для настройки своей семьи.
- 6 Следуйте инструкциям, выводимым на экран.

Добавление ребенка в учетную запись

При добавлении каждого ребенка родительский контроль применяет predetermined домашние правила в зависимости от возраста детей. Вы можете скорректировать эти домашние правила в любой момент в соответствии с индивидуальным уровнем развития ребенка.

Примечание: Можно добавить до 15 детей в свою учетную запись. Можно в любое время удалить или добавить ребенка из вашей учетной записи Norton Family.

- 1 В поле **Имя ребенка** введите имя ребенка.

Примечание: Имя не должно содержать специальные символы, такие как &, # и \$.

- 2 Выберите год рождения ребенка.
Домашние правила применяются исходя из возраста ребенка.
- 3 Нажмите **Выбрать аватар** или **Загрузить фотографию** для установки изображения профиля для вашего ребенка.

Примечание: Вы можете добавить других детей в свою учетную запись после завершения настройки для первого ребенка.

- 4 Нажмите **Далее**.

Установка Norton Family на устройстве ребенка

Установите Norton Family на всех устройствах, используемых ребенком. Если вы в данный момент не используете устройство ребенка, нажмите **Нет**, чтобы отправить ссылку для загрузки по электронной почте. Откройте это сообщение электронной почты на устройстве, на котором требуется установить Norton Family.

Как установить Norton Family в Windows

- 1 В разделе **Использует ли ваш ребенок это устройство?**, нажмите кнопку **Да** и затем нажмите кнопку **Далее**.
- 2 Нажмите или запустите загруженный файл программы установки.
- 3 Диспетчер загрузки Norton автоматически установит Norton Family на устройство.
- 4 Прочитайте лицензионное соглашение с пользователем, а затем нажмите **Принять и установить**.
Устройство будет автоматически связано с вашей учетной записью.
- 5 Нажмите кнопку **Продолжить**.
- 6 В окне назначения устройств нажмите **Изменить** рядом с именем ребенка, которому требуется назначить данное устройство.
- 7 Нажмите **Входит в систему под именем** и выберите учетную запись, применяемую ребенком для входа на устройство. Если ребенок пользуется несколькими учетными записями, выберите этого ребенка в каждой из них.
- 8 Нажмите **Сохранить > ОК**.

Как установить приложение Norton Family на устройстве Android

- 1 В окне **УСТАНОВИТЬ Norton Family** нажмите **Да**, затем нажмите **Продолжить**.
- 2 Нажмите **Загрузить приложение Norton Family**.
- 3 Если появится соответствующий запрос, выполните действие при помощи **Play Store**.
- 4 Нажмите **Установить** и следуйте инструкциям на экране.
- 5 Откройте приложение Norton Family для родительского контроля.
- 6 Ознакомьтесь с текстом **Лицензионного соглашения Norton** и коснитесь кнопки **Принять и продолжить > С чего начать**.
- 7 Нажмите **Вход** и введите данные учетной записи.
- 8 Коснитесь пункта **Ребенок**, чтобы включить режим ребенка, а затем коснитесь кнопки **Продолжить**.
В режиме ребенка можно добавить ребенка и назначить домашние правила для этого устройства.
- 9 Чтобы добавить ребенка, коснитесь пункта **Добавить ребенка** и в окне **ПРОФИЛЬ** введите сведения о ребенке.
Коснитесь изображения, чтобы выбрать аватар для профиля ребенка. Для профиля ребенка можно выбрать изображение из фотогалереи либо сделать снимок.

- 10 Коснитесь пункта **Продолжить**, а затем — **Сохранить**.

Norton Family устанавливает домашние правила по умолчанию исходя из возраста ребенка. Для просмотра правил, назначенных ребенку, коснитесь пункта **Домашние правила**.

- 11 Выберите ребенка, которому вы хотите назначить это устройство, введите имя, с помощью которого вы будете определять устройство, затем нажмите **Готово**.
- 12 Если появится соответствующий запрос, включите параметры **Использование приложения** и **Специальные возможности**.
- 13 В появившемся предупреждении нажмите **Активировать**, чтобы настроить приложение Norton Family в качестве администратора устройства.

Как установить приложение Norton Family на устройстве iOS

- 1 В окне **УСТАНОВИТЬ Norton Family** нажмите **Да**, затем нажмите **Продолжить**.

2 Нажмите **Загрузить приложение Norton Family**.

3 Нажмите и установите приложение **Norton Family**.

4 Нажмите **Открыть**.

5 Нажмите **ОК**, чтобы разрешить Norton Family отправлять вам уведомления.

6 Ознакомьтесь с **лицензионным соглашением Norton** и **политикой конфиденциальности** и затем нажмите **Принять и продолжить**.

7 Войдите, используя свою учетную запись.

8 На экране **Добавить ребенка** введите сведения о ребенке и нажмите **Добавить**.

Чтобы добавить еще одного ребенка, нажмите **Добавить нового ребенка** и в окне **Добавить ребенка** введите сведения о ребенке и нажмите **Добавить**.

Коснитесь изображения, чтобы выбрать аватар для профиля ребенка. Для профиля ребенка можно выбрать изображение из фотогалереи либо сделать снимок.

9 Выберите ребенка, которому вы хотите назначить это устройство, и введите имя, с помощью которого вы будете определять устройство.

10 Нажмите **Назначить**.

11 Нажмите **Установить** и следуйте инструкциям на экране, чтобы установить профиль.

Установка профиля требуется для работы мгновенной блокировки и других компонентов на устройстве ребенка.

12 Следуйте выводимым на экран инструкциям, чтобы настроить ограничения.

Установка Norton Family на устройстве родителя

После завершения установки необходимо загрузить и установить следующее приложение на вашем мобильном устройстве:

- Устройство Android: установите приложение **Norton Family для родительского контроля**
- Устройство iOS: установите приложение **Norton Family для родителей**

Загрузка и установка приложения Norton Family для родительского контроля на Android

- 1 Запустите приложение Play Store и введите в строку поиска слова **родительский контроль Norton Family**.
- 2 Выберите приложение **Norton Family для родительского контроля** и нажмите **Установить**.
- 3 По окончании установки откройте приложение.
- 4 Прочитайте **Лицензионное соглашение Norton** и другие политики, а затем нажмите **Принять**.
- 5 Войдите, используя свою учетную запись.
- 6 Нажмите **Устройство родителя**. Если вы используете устройство вместе с ребенком, переключитесь в **Режим ребенка**, прежде чем передать устройство вашему ребенку.

Загрузка и установка приложения Norton Family для родительского контроля на iOS

- 1 Запустите приложение App Store и введите в строку поиска слова **Norton Family для родителей**.
- 2 Выберите приложение **Norton Family для родителей**, затем нажмите **Получить**.
- 3 По окончании установки откройте приложение.
- 4 Прочитайте **Лицензионное соглашение Norton** и другие политики, а затем нажмите **Принять**.
- 5 Войдите, используя свою учетную запись.

Расскажите об этом членам своей семьи

Общение — это основа безопасности семьи в Интернете. Поговорите с ребенком, объяснив важность ответственного подхода к использованию Интернета.

Защитите свою банковскую информацию с помощью Norton Safe Web

Защита банковских операций в Norton Safe Web обеспечивает повышенную безопасность при работе с банковскими веб-сайтами. При доступе к банковскому веб-сайту с помощью браузера Google Chrome, Mozilla Firefox или Microsoft Edge вы получаете уведомление о необходимости установить или включить расширение Norton Safe Web. Нажмите **Установить** или **Включить** в уведомлении и следуйте инструкциям на экране, чтобы установить или включить расширение Norton Safe Web.

Вы можете отключить уведомление о защите банковских операций, нажав **Больше не показывать** в уведомлении или при переходе к окну **Настройки**.

Включение и выключение уведомлений о защите банковских операций

1 Запустите Norton.

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

2 В главном окне продукта Norton щелкните **Параметры**.

3 В окне **Параметры** нажмите **Брандмауэр**.

4 На вкладке **Вторжения и защита браузера** в строке **Уведомления защиты банковских операций** переместите переключатель **Вкл. / Выкл.** в положение **Выкл.** или **Вкл.**

5 В окне **Параметры** нажмите кнопку **Применить**, а затем — кнопку **Заккрыть**.

Управление безопасностью устройства

В этой главе рассмотрены следующие вопросы:

- [Что делать, если устройство находится под угрозой](#)
- [Используйте Norton для оптимизации и повышения производительности компьютера](#)
- [Запуск сканирования Norton для обнаружения угроз на ПК](#)
- [Защитите свое устройство от эксплойтов, хакеров и атак нулевого дня](#)
- [Настройте Norton, чтоб отслеживать приложения и запретить доступ к вашему компьютеру вредоносным веб-сайтам](#)
- [Начало использования резервного копирования в облаке Norton](#)
- [Настройка параметров продукта Norton](#)
- [Оптимизация компьютера для игр при помощи Game Optimizer](#)

Что делать, если устройство находится под угрозой

Цвет плиток «Безопасность», «Безопасность в Интернете», «Резерв. копир.» и «Быстродействие» в главном окне продукта Norton указывает состояние каждой категории, например:

- **Зеленый** : защита включена.
- **Оранжевый** : компьютер требует внимания.
- **Красный** : ваш компьютер под угрозой.

Примечание: Категория «Резерв. копия» доступна только для подписок Deluxe, Premium и Norton 360.

Norton автоматически исправляет большинство проблем, способных ослабить защиту или снизить быстродействие системы, и отображает состояние Защищено в главном окне. Проблемы, требующие внимания пользователя, отмечаются Norton как **Под угрозой** или **Внимание**.

Реагирование на индикаторы состояния "Внимание" и "Под угрозой"

1 Запустите Norton.

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

2 В главном окне продукта Norton выберите категорию, отмеченную красным или оранжевым цветом, который означает состояние **Под угрозой** или **Внимание**.

3 Нажмите кнопку **Исправить** и следуйте инструкциям, выводимым на экран.

Если проблему не удалось исправить, выберите **Справка > Получить поддержку**, чтобы запустить инструмент диагностики.

Если есть основания полагать, что компьютер серьезно заражен, можно воспользоваться [средствами Norton Rescue](#).

Запуск LiveUpdate

Компания NortonLifeLock рекомендует запускать LiveUpdate с регулярными интервалами в указанных ниже случаях.

- Если выключен параметр **Автоматический запуск LiveUpdate**.
- Если компьютер в течение длительного времени не подключен к Интернету.

Примечание: Чтобы запустить LiveUpdate, необходима действующая подписка и подключение к Интернету.

Запуск LiveUpdate вручную

- 1 Запустите Norton.
Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.
- 2 В главном окне продукта Norton дважды щелкните **Безопасность**, а затем выберите **LiveUpdate**.
- 3 После успешного завершения работы LiveUpdate в окне **Norton LiveUpdate** нажмите **ОК**.

Просмотр и исправление угроз безопасности устройства, обнаруженных Norton

При обнаружении Norton угрозы безопасности программа автоматически удаляет ее, за исключением случаев, когда ваше вмешательство необходимо для определения способа обработки угрозы. В таких случаях Norton отображает уведомление «Обнаружены угрозы» или «Угроза безопасности» с доступными вариантами реакции на угрозу безопасности.

Просмотр угроз, которые были автоматически устранены во время сканирования

- 1 Запустите Norton.
Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.
- 2 В главном окне Norton дважды щелкните **Безопасность**, а затем выберите **Журнал**.
- 3 В окне **Журнал безопасности** в списке **Показать** выберите пункт **Устраненные угрозы безопасности**.
- 4 Выберите угрозу в списке и просмотрите выполненные действия на панели **Сведения**.

Исправление угроз, которые не были устранены во время сканирования

В некоторых случаях вместо автоматического устранения угрозы Norton рекомендует вам выполнить определенное действие для ее устранения.

Исправление угроз, которые не были устранены во время сканирования

- 1 Запустите Norton.
Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.
- 2 В главном окне Norton дважды щелкните **Безопасность**, а затем выберите **Журнал**.

- 3 В окне **Журнал безопасности** в списке **Показать** выберите пункт **Неустраненные угрозы безопасности**.
- 4 Если список содержит неустраненные угрозы, выберите интересующую вас угрозу.
- 5 Выполните **рекомендуемые действия**, указанные на панели **Сведения**.

Примечание: После того как Norton удалит угрозу безопасности, иногда может потребоваться перезапуск компьютера. Если Norton предложит перезапустить компьютер, сохраните все открытые файлы и перезапустите компьютер.

Примечание: Если есть основания полагать, что система заражена, запустите Norton Power Eraser. Norton Power Eraser — это мощное средство удаления вредоносных программ, позволяющее избавиться от наиболее устойчивых к удалению угроз безопасности. Дополнительную информацию см. в разделе См. "[Запуск сканирования Norton для обнаружения угроз на ПК](#)" на стр. 37.

Действия при помещении рисков или угроз в карантин

Элементы, помещенные в карантин, не могут распространяться или заражать компьютер. Если какой-либо элемент, который, по вашему мнению, заражен, но при этом не идентифицирован продуктом Norton как содержащий угрозу, вы можете поместить этот элемент в карантин вручную. Вы также можете восстановить элемент из карантина, если считаете, что он отличается низким уровнем угрозы. Norton не исправляет элементы, которые вы восстанавливаете. Однако Norton может удалить угрозу из восстановленных элементов во время последующих проверок.

Восстановление элемента из карантина

- 1 Запустите Norton.
 Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.
- 2 В главном окне Norton дважды щелкните **Безопасность**, а затем выберите **Журнал**.
- 3 В окне **Журнал безопасности** в раскрывающемся списке **Показать** выберите категорию **Карантин**.
- 4 Выберите элемент, которым вы хотите управлять.
- 5 На панели **Сведения** щелкните **Параметры**.
 Перейдя по ссылке **Дополнительные настройки**, можно просмотреть дополнительную информацию об объекте перед выбором действия для него. Ссылка открывает окно **File Insight**, содержащее подробное описание угрозы.
- 6 В окне **Обнаружена угроза** выберите один из следующих вариантов:

- **Восстановить** : возвращает элементы в исходное расположение на компьютере. Этот вариант доступен только для элементов, помещенных в карантин вручную.
 - **Восстановить и исключить этот файл** : это действие возвращает помещенный в карантин элемент в исходное расположение без исправления и исключает его из будущих операций сканирования. Этот параметр доступен для обнаруженных угроз, как являющихся, так и не являющихся вирусами.
 - **Удалить из журнала** : удаляет выбранный элемент из **Журнала безопасности**.
- 7 В окне **Восстановление из карантина** нажмите кнопку **Да**.
 - 8 В окне **Обзор папок** выберите папку или диск для размещения восстановленного файла и нажмите кнопку **ОК**.

Восстановление файла, который был ошибочно распознан как угроза безопасности

По умолчанию Norton удаляет угрозы безопасности с компьютера и помещает их в карантин. Если есть основания полагать, что файл был удален по ошибке, то его можно восстановить из карантина в исходном расположении и исключить из последующих операций сканирования.

Восстановление файла из карантина

Примечание: Исключайте программу из операций сканирования Norton только в том случае, если уверены в ее безопасности. Например, программу, представляющую угрозу, можно сохранить, если от нее зависит работа нужной программы.

- 1 Запустите Norton.
Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.
- 2 В главном окне Norton щелкните **Безопасность**, а затем выберите **Журнал**.
- 3 В окне **Журнал безопасности** раскройте меню **Показать** и выберите вариант **Карантин**.
- 4 Выберите файл, который необходимо восстановить.
- 5 На панели **Сведения** щелкните **Параметры**.
- 6 В окне **Обнаружена угроза** выберите команду **Восстановить и исключить этот файл**.

- 7 В окне **Восстановление из карантина** нажмите кнопку **Да**.
- 8 В окне **Найти папку** выберите папку или диск для размещения восстановленного файла и нажмите кнопку **ОК**.

Отправить элемент для дальнейшего анализа Norton

Вы можете повысить эффективность своего продукта Norton, отправив файлы, которые, по вашему мнению, представляют угрозу безопасности. Norton Security Response анализирует файл и, если он представляет угрозу безопасности, добавляет его в будущие описания защиты.

Примечание: Вместе с файлами не отправляется никакая личная информация.

- 1 Запустите Norton.
Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.
- 2 В главном окне Norton дважды щелкните **Безопасность**, а затем выберите **Журнал**.
- 3 В окне **Журнал безопасности** в раскрывающемся списке **Показать** выберите категорию **Карантин**.
- 4 Выберите элемент, которым вы хотите управлять.
- 5 На панели **Сведения** щелкните **Параметры**.
Перейдя по ссылке **Дополнительные настройки**, можно просмотреть дополнительную информацию об объекте перед выбором действия для него. Ссылка открывает окно **File Insight**, содержащее подробное описание угрозы.
- 6 В окне **Обнаружена угроза** выберите команду **Отправить в NortonLifeLock**.
- 7 На открывшемся экране нажмите кнопку **ОК**.

Помещение элемента в карантин вручную

- 1 Запустите Norton.
Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.
- 2 В главном окне Norton дважды щелкните **Безопасность**, а затем выберите **Журнал**.
- 3 В окне **Журнал безопасности** в раскрывающемся списке **Показать** выберите категорию **Карантин**.

- 4 Нажмите **Поместить в карантин**.
- 5 В окне **Добавление в карантин вручную** добавьте файл, который хотите поместить в карантин, и введите описание для справки.

Примечание: Если вы помещаете в карантин файл, связанный с какими-либо запущенными процессами, то эти процессы завершаются. Поэтому закройте все открытые файлы и запущенные процессы, прежде чем добавлять файл в карантин.

Используйте Norton для оптимизации и повышения производительности компьютера

Мы знаем, как это неприятно, когда компьютер работает медленно, а простые задачи выполняются целую вечность. Многим пользователям кажется, что после установки Norton производительность компьютера снижается. На самом деле это наоборот. Norton не только обеспечивает первоклассную защиту вашего компьютера без снижения производительности,

но и может повысить скорость его работы за счет использования инструментов управления производительностью и оптимизации, которые ускоряют выполнение повседневных задач.

Ускорение загрузки компьютера

Многие приложения запускаются одновременно с компьютером. К ним относятся программы, которые вы редко используете или вообще не используете. Вы можете даже не знать, что на вашем компьютере есть такие программы. Чем больше программ, которые запускаются при загрузке компьютера, тем дольше она выполняется. **Norton Startup Manager** позволяет отключить или отложить запуск программ, чтобы ускорить работу компьютера.

Включение или откладывание запуска элементов автозагрузки

- 1 Запустите Norton.
 - Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.
- 2 В главном окне Norton дважды щелкните **Быстродействие** и выберите **Диспетчер автозагрузки**.
- 3 В окне **Диспетчер автозагрузки** выполните следующее:
 - В столбце **Вкл/Выкл** снимите флажки рядом с неиспользуемыми программами для того, чтобы они не запускались при загрузке компьютера.

- В столбце **Задержка запуска** выберите программы, которые необходимо запускать только после завершения загрузки.

4 Нажмите кнопку **Применить**, а затем — кнопку **Заккрыть**.

Сокращение времени загрузки программ и файлов

Инструмент **оптимизации диска** упорядочивает фрагменты файлов, рассеянные по системе компьютера. Он повышает быстродействие компьютера, что позволяет вам работать более эффективно.

Выполнение оптимизации диска

1 Запустите Norton.

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

2 В главном окне Norton дважды щелкните **Быстродействие**, а затем выберите **Оптимизировать диск**.

3 По завершении работы нажмите **Заккрыть**.

Удаление временных файлов и папок, замедляющих работу компьютера

Каждый раз при просмотре страниц в Интернете или загрузке файлов компьютер сохраняет в системе временные файлы. Со временем этих ненужных файлов становится все больше и больше, и они могут замедлить работу компьютера. Инструмент очистки файлов удаляет весь мусор, чтобы компьютер работал быстрее.

Удаление временных файлов и папок

1 Запустите Norton.

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

2 В главном окне Norton дважды щелкните **Быстродействие**, затем выберите **Очистка файлов**.

3 По завершении работы нажмите **Заккрыть**.

Оптимизация загрузочного тома

Оптимизация загрузочного тома позволяет увеличить объем практически доступного свободного места путем переупорядочивания фрагментов файлов в последовательно расположенные цепочки кластеров. Если головка жесткого диска может прочитать все данные файла из одного расположения, скорость чтения файла в память возрастает.

Оптимизация загрузочного тома

- 1 Запустите Norton.

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

- 2 В главном окне Norton дважды щелкните **Быстродействие** и выберите **Графики**.
- 3 В окне **Графики** в верхней части графика состояния безопасности щелкните **Оптимизация**.

Повышение производительности во время прохождения игр или просмотра фильмов

Запускалось ли программное обеспечение безопасности во время того, как вы играли в игру или смотрели фильм, и при этом экран переставал отвечать в самый неудобный момент? Вы можете настроить параметр **Распознавание полноэкранного режима**, чтобы выполнение текущей программы не прерывалось. В этом случае продукт Norton будет запускать фоновые задачи для обеспечения защиты после того, как вы завершите работу с приложением.

Убедитесь, что параметр **Распознавание полноэкранного режима** включен

- 1 Запустите Norton.

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

- 2 В главном окне Norton щелкните **Параметры**.
- 3 В окне **Параметры** нажмите **Параметры администрирования**.
- 4 В разделе **Параметры режима без вывода сообщений** найдите строку **Распознавание полноэкранного режима** и переместите выключатель в положение **Вкл**.
- 5 Нажмите кнопку **Применить**, а затем — кнопку **Заккрыть**.

Никаких перерывов при использовании любимых приложений

Если вы считаете, что продукт Norton замедляет работу ваших любимых программ, воспользуйтесь параметром **Тихий режим**, который не позволит продукту Norton запускаться во время их использования. В этом случае продукт Norton будет запускать фоновые задачи для обеспечения защиты после того, как вы завершите работу с такими программами.

Запуск любимых программ в тихом режиме

- 1 Запустите Norton.

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

- 2 В главном окне Norton щелкните **Параметры**.
- 3 В окне **Параметры** нажмите **Параметры администрирования**.
- 4 В окне **Параметры режима без вывода сообщений** найдите строку **Пользовательские программы** и нажмите **Настроить**.
- 5 В окне **Программы тихого режима** нажмите **Добавить**.
- 6 В диалоговом окне **Добавить программу** перейдите к необходимой программе.
- 7 Выберите файл, нажмите **Открыть**, а затем — **ОК**.

Отображать программы, расходующие ресурсы и замедляющие работу

Norton отслеживает состояние компьютера и может предупредить вас в случае, когда программа или процесс использует необычный объем ресурсов. Если вы не используете эти программы, их можно закрыть, чтобы повысить производительность.

Определять процессы, расходующие ресурсы

- 1 Запустите Norton.

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

- 2 В главном окне Norton дважды щелкните **Быстродействие** и выберите **Графики**.
- 3 На левой панели окна **Графики** щелкните **Использование**.
- 4 Выполните одно из следующих действий:
 - Для просмотра графика использования процессора перейдите на вкладку **ЦП**.

- Для просмотра графика памяти перейдите на вкладку **Память**.
- 5 Щелкните на произвольной точке графика для просмотра списка процессов с максимальным расходом ресурсов.
- Щелкните на имени процесса, чтобы получить дополнительную информацию о нем в окне **File Insight**.

Запуск сканирования Norton для обнаружения угроз на ПК

Norton автоматически обновляет описания вирусов и регулярно проверяет компьютер на наличие различных угроз. Если компьютер был отключен от сети или на нем мог появиться вирус, вы можете выполнить различные проверки вручную:

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

Примечание: Первое сканирование после установки Norton может занять час или больше в связи с первоначальным анализом системы.

Быстрое сканирование, полное сканирование системы или сканирование по требованию

- 1 Запустите Norton.
Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.
- 2 В главном окне Norton дважды щелкните **Безопасность**, а затем выберите **Сканирования**.
- 3 В окне **Операции сканирования** рядом с полем **Сканирования и задачи** выберите один из следующих пунктов:
 - **Быстрое сканирование** > **Перейти**
 - **Полное сканирование системы** > **Перейти**

- **Выборочное сканирование** > **Перейти**, затем нажмите **Запустить** рядом с пунктом **Сканирование дисков**, **Сканирование папок** или **Сканирование файлов**, чтобы перейти к компонентам, которые необходимо просканировать.
- 4 В окне **Обзор результатов** нажмите **Готово**.
- Если такие записи есть, просмотрите угрозы в окне **Обнаруженные угрозы**.

Полное сканирование системы

Функция полного сканирования тщательно проверяет систему, чтобы удалить вирусы и другие угрозы безопасности. В ходе такого сканирования проверяются все загрузочные записи, файлы и активные процессы, доступ к которым предоставлен пользователю. Компьютер сканируется более тщательно, и это занимает больше времени.

Примечание: При полном сканировании системы, запущенном администратором, обрабатывается больше файлов, чем при сканировании с использованием учетной записи обычного пользователя.

Выполнение полного сканирования системы

- 1 Запустите Norton.
Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.
- 2 В главном окне Norton дважды щелкните **Безопасность**, а затем выберите **Сканирования**.
- 3 В окне **Операции сканирования** в разделе **Сканирования и задачи** щелкните **Полное сканирование**.
- 4 Нажмите кнопку **Перейти**.

Выборочное сканирование

В ходе работы может потребоваться выполнить сканирование отдельного файла, съемного диска, жесткого диска, папки или файла компьютера. Например, если вы работаете со съемным диском и подозреваете наличие на нем вируса, то можете просканировать только этот диск. Также, если вы получили сжатый файл по электронной почте и подозреваете, что файл заражен вирусом, то можете просканировать этот файл.

Сканирование отдельных элементов

1 Запустите Norton.

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

2 В главном окне Norton дважды щелкните **Безопасность**, а затем выберите **Сканирования**.

3 В окне **Операции сканирования** в разделе **Сканирования и задачи** щелкните **Выборочное сканирование**.

4 Нажмите кнопку **Перейти**.

5 В окне **Операции сканирования** выполните одно из следующих действий:

- Чтобы просканировать определенные диски, нажмите кнопку **Запустить** рядом с пунктом **Сканировать диски**, выберите диски, которые требуется просканировать, а затем нажмите кнопку **Сканировать**.
- Чтобы просканировать определенные папки, нажмите кнопку **Запустить** рядом с пунктом **Сканировать папки**, выберите папки, которые требуется просканировать, а затем нажмите кнопку **Сканировать**.
- Чтобы просканировать определенные файлы, нажмите кнопку **Запустить** рядом с пунктом **Сканировать файлы**, выберите файлы, которые требуется просканировать, а затем нажмите кнопку **Добавить**. Нажав клавишу **Ctrl**, можно выбрать несколько файлов для включения в план сканирования.

6 В окне **Обзор результатов** нажмите **Готово**.

Если есть элементы, требующие внимания, просмотрите их и примите рекомендуемые меры.

Сканирование Norton Power Eraser

Norton Power Eraser — это мощное средство удаления вредоносных программ, которое может помочь избавиться от сложных для удаления угроз безопасности. В отличие от обычных процессов сканирования Norton Power Eraser использует более агрессивные методы. При этом существует риск, что Norton Power Eraser пометит безопасную программу для удаления. Перед удалением любых файлов с помощью Norton Power Eraser внимательно проверьте результаты сканирования.

Загрузка Norton Power Eraser и выполнение сканирования (в Windows 10/8/7)

1 Загрузите [Norton Power Eraser](#).

2 Нажмите **Ctrl + J**, чтобы открыть окно **Загрузки** в браузере, и дважды щелкните файл **NPE.exe**.

Если отобразится окно Контроль учетных записей, нажмите **Да** или **Продолжить**.

- 3 Прочитайте лицензионное соглашение и нажмите **Принять**.
Если вы уже приняли лицензионное соглашение, этот запрос больше не появится.
Norton Power Eraser проверяет наличие новой версии и автоматически загружает ее.
- 4 В окне Norton Power Eraser выберите **Полное сканирование** и нажмите **Выполнить**.
- 5 Если вы хотите выполнить сканирование на наличие руткитов, нажмите **Параметры** и в разделе **Параметры сканирования и журналов** включите параметр **Включить сканирование на руткиты (требуется перезагрузки компьютера)** и нажмите **Применить**.
- 6 Когда отобразится запрос перезагрузки компьютера, нажмите **Перезагрузить**.
Дождитесь завершения сканирования. Следуйте инструкциям на экране.

Загрузка Norton Power Eraser и выполнение сканирования (в Windows XP/Vista)

- 1 Загрузите [Norton Power Eraser](#).
- 2 Нажмите **Ctrl + J**, чтобы открыть окно **Загрузки** в браузере, и дважды щелкните файл **NPE.exe**.
Если отобразится окно Контроль учетных записей, нажмите **Да** или **Продолжить**.
- 3 Прочитайте лицензионное соглашение и нажмите **Принять**.
Norton Power Eraser проверяет наличие новой версии и предлагает загрузить ее, если она доступна.
- 4 В окне **Norton Power Eraser** щелкните **Сканировать на наличие угроз**.
- 5 По умолчанию Norton Power Eraser выполняет сканирование на наличие руткитов и требует перезапуска системы. Когда отобразится запрос перезагрузки компьютера, нажмите **Перезагрузить**.
Если сканирование на наличие руткитов не требуется, перейдите в раздел **Параметры** и снимите флажок **Включить сканирование на наличие руткитов (требуется перезагрузки компьютера)**.
- 6 Дождитесь завершения сканирования. Следуйте инструкциям на экране.

Создавайте собственные выборочные сканирования Norton

Параметры автоматического сканирования подходят для большинства пользователей, однако некоторые пользователи предпочитают настраивать параметры для сканирования определенных дисков, папок и файлов по выбранному ими расписанию.

Создание выборочного сканирования

1 Запустите Norton.

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

2 В главном окне Norton дважды щелкните **Безопасность**, а затем выберите **Сканирования**.

3 В окне **Операции сканирования** в разделе **Сканирования и задачи** выберите пункт **Пользовательское сканирование**, а затем нажмите **Перейти**.

4 В окне **Сканирование** выберите **Создать сканирование**.

5 В окне **Новое сканирование** введите название в поле **Имя сканирования** и добавьте следующие параметры:

- На вкладке **Элементы сканирования** нажмите **Добавить диски**, **Добавить папки** или **Добавить файлы**, чтобы перейти к компонентам, которые вы хотите включить в сканирование.
- На вкладке **Запланировать сканирование** разделе «Когда требуется выполнять сканирование?» выберите интервал, а затем временные параметры. Выберите параметры в разделе **Запускать сканирование**. Для большинства пользователей лучше оставить все флажки установленными. При этом сканирование будет запускаться только тогда, когда вы не используете компьютер и когда он работает от сети, а не от батареи; компьютер не перейдет в режим сна во время сканирования.
- На вкладке **Параметры сканирования** с помощью переключателей задайте поведение сжатых файлов и угроз с низким уровнем риска в ходе сканирования.

6 Нажмите кнопку **Сохранить**.

Изменение и удаление выборочного сканирования Norton

Ранее созданное выборочное сканирование можно изменить. При изменении можно переименовать сканирование, добавить или исключить файлы, а также изменить расписание. Если сканирование больше не нужно, его можно удалить.

Изменение и удаление выборочного сканирования

1 Запустите Norton.

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

2 В главном окне Norton дважды щелкните **Безопасность**, а затем выберите **Сканирования**.

- 3 В окне **Операции сканирования** в разделе **Сканирования и задачи** выберите пункт **Пользовательское сканирование**, а затем нажмите **Перейти**.
- 4 В окне **Сканирование** в столбце **Изменить параметры сканирования** рядом с операцией выборочного сканирования, параметры которой нужно изменить выполните одно из следующих действий:
 - Нажмите значок изменения, и в появившемся окне **Изменить сканирование** с помощью переключателей включите или отключите необходимые функции. Для большинства пользователей подходят параметры по умолчанию. Нажмите **Использовать параметры по умолчанию**, чтобы удалить пользовательские настройки.
 - Нажмите значок корзины, а затем для подтверждения удаления выборочного сканирования нажмите кнопку **Да**.
- 5 Нажмите кнопку **Сохранить**.

Планирование сканирования Norton

Norton определяет, когда вы находитесь вдали от компьютера, и автоматически запускает сканирование, чтобы обеспечить регулярный мониторинг вашей системы на наличие угроз. Также вы можете самостоятельно запланировать быстрое сканирование, полное сканирование системы или выборочное сканирование в удобное для вас время.

Планирование быстрого сканирования Norton, полного сканирования системы или выборочного сканирования

- 1 Запустите Norton.

Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.
- 2 В главном окне Norton дважды щелкните **Безопасность**, а затем выберите **Сканирования**.
- 3 В окне **Операции сканирования** в разделе **Сканирования и задачи** щелкните **Выборочное сканирование**.
- 4 Нажмите кнопку **Перейти**.
- 5 В окне **Сканирование** в столбце **Изменить сеанс сканирования** щелкните по значку рядом с быстрым сканированием, полным сканированием системы или выборочным сканированием, созданным вами.
- 6 В окне **Изменить параметры сканирования** откройте вкладку **Расписание сканирования** и выполните одно из следующих действий:
 - В разделе **Когда требуется выполнять сканирование?** выберите интервал, а затем временные параметры.

- Выберите параметры в разделе **Запускать сканирование**. Для большинства пользователей лучше оставить все флажки установленными. При этом сканирование будет запускаться только тогда, когда вы не используете компьютер и когда он работает от сети, а не от батареи; компьютер не перейдет в режим сна во время сканирования.
- 7 Нажмите кнопку **Далее**.
 - 8 В окне **Параметры сканирования** нажмите кнопку **Сохранить**.

Просмотр угроз в реальном времени, обнаруженных Norton SONAR

SONAR обеспечивает защиту в реальном времени от угроз и выполняет превентивный поиск неизвестных угроз безопасности. SONAR распознает новые угрозы, исходя из поведения приложений. Этот метод работает быстрее, чем традиционное обнаружение угроз на базе сигнатур. Данная технология защищает компьютер от вредоносного кода еще до того, как описания вирусов станут доступны в LiveUpdate.

Примечание: Защита SONAR всегда должна быть включена. Система SONAR отключена, если выключена функция автоматической защиты, и ваш компьютер не защищен от возникающих угроз.

Просмотр рисков, обнаруженных SONAR

- 1 Запустите Norton.
Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.
- 2 В главном окне Norton дважды щелкните **Безопасность**, а затем выберите **Журнал**.
- 3 В окне **Журнал безопасности** в раскрывающемся списке выберите пункт **Операции SONAR**.
- 4 Если список содержит угрозы, выберите интересующую вас угрозу.
- 5 Выполните **Рекомендуемое действие**, указанное на панели **Сведения**.
В этой категории также показаны все операции по изменению конфигурации или параметров компьютера. С помощью параметра **Дополнительные сведения** в этой категории можно просмотреть подробные сведения о ресурсах, измененных в ходе операции.

Проверка включения защиты SONAR

- 1 Запустите Norton.
Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.
- 2 В главном окне Norton щелкните **Параметры**.
- 3 В окне **Параметры** выберите **Защита от вирусов**.
- 4 На вкладке **Автоматическая защита** в разделе **Защита в реальном времени** переместите переключатель **Защита SONAR** в положение **Вкл**.
- 5 Нажмите кнопку **Применить**.
- 6 В окне **Параметры** нажмите кнопку **Закрыть**.

Исключение файлов и папок из сканирований автоматической защиты Norton, SONAR и контроля загрузок

Можно настроить Norton таким образом, чтобы исключить определенные программы из процедур сканирования функциями автоматической защиты и SONAR. Окна **Исключения из сканирования** и **Исключения в режиме реального времени** позволяют исключить вирусы и прочие серьезные угрозы безопасности. Файл или папка, добавленные в список исключений, будут игнорироваться Norton при выполнении сканирования.

Чтобы исключить файл из контроля загрузок, необходимо выбрать папку и загрузить в нее файл. Например, при загрузке небезопасного исполняемого файла в эту папку Norton позволяет загрузить его и не удаляет его с компьютера. Необходимо создать новую папку специально для исключений функции контроля загрузок.

Примечание: Исключать файл из сканирований, выполняемых Norton, следует только в случае крайней необходимости, поскольку такие действия снижают уровень защиты компьютера. Исключайте только те элементы, про которые вы точно знаете, что они не заражены.

Исключение из сканирования серьезных угроз безопасности

- 1 Запустите Norton.
Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.
- 2 В главном окне Norton щелкните **Параметры**.
- 3 В окне **Параметры** выберите **Защита от вирусов**.
- 4 В окне параметров **Антивирусная программа** откройте вкладку **Сканирования и угрозы**.

- 5 В разделе **Исключения / Угрозы с низкой степенью риска** выполните одно из следующих действий:
 - В строке **Элементы, исключаемые из сканирования** нажмите кнопку **Настроить**.
 - В строке **Элементы для исключения из сканирований автоматической защиты, управления сценариями, SONAR и контроля загрузок** нажмите кнопку **Настроить**.
- 6 В открывшемся окне выберите **Добавить папки** или **Добавить файлы**.

Исключения можно назначить для локальных дисков, папок, групп файлов, отдельных файлов, а также сетевых дисков. Однако Norton не поддерживает исключение файлов, расположенных в сети. Если в список исключений добавляется сетевой диск, убедитесь, что он подключен к компьютеру.
- 7 В окне **Добавить элемент** щелкните по значку обзора.
- 8 В открывшемся окне выберите объект, который требуется исключить из сканирования.

При добавлении папок можно указать, следует ли включать в него вложенные папки.
- 9 Нажмите кнопку **ОК**.
- 10 В окне **Добавить элемент** нажмите кнопку **ОК**.
- 11 В открывшемся окне нажмите кнопку **Применить**, а затем — **ОК**.

Исключение файлов с сигнатурами низкой степени риска из сканирований Norton

Исключения сигнатур Norton позволяют выбрать отдельные угрозы безопасности, которые следует исключить из операций сканирования продукта Norton. Например, легальное приложение — например, бесплатная игра — может поставляться в комплекте с другой программой, например, программой показа объявлений. При этом вы можете оставить программу показа рекламы, даже несмотря на то, что она подвергает вас риску. Исключив ее из сканирования, можно избежать просмотра предупреждений о наличии этой программы при последующих сканированиях.

Примечание: Настройка исключений ослабляет защиту и должна применяться только в случае крайней необходимости, в случае, если вы осознаете все потенциальные риски, связанные с исключением известных угроз из сканирований Norton.

Добавление сигнатуры с низкой степенью риска в список исключения сигнатур

- 1 Запустите Norton.
Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.
- 2 В главном окне Norton щелкните **Параметры**.
- 3 В окне **Параметры** выберите **Защита от вирусов**.
- 4 В окне параметров **Антивирусная программа** откройте вкладку **Сканирования и угрозы**.
- 5 В разделе **Исключения / Угрозы с низкой степенью риска** в строке **Сигнатуры, исключаемые из всех процедур обнаружения** щелкните **Настроить**.
- 6 В окне **Исключения сигнатур** нажмите кнопку **Добавить**.
- 7 В окне **Угрозы безопасности** щелкните угрозу, которую требуется исключить, и нажмите кнопку **Добавить**.
- 8 В окне **Исключения сигнатур** нажмите кнопку **Применить**, а затем — **ОК**.

Включение и выключение автоматических задач

Работая в фоновом режиме, Norton выполняет автоматические задачи для защиты компьютера. Эти автоматические задачи включают сканирование на наличие вирусов, мониторинг подключения к Интернету, загрузку обновлений защиты и другие важные действия. Эти операции выполняются в фоновом режиме, когда компьютер включен.

Если какой-нибудь элемент требует вашего внимания, Norton отображает сообщение со сведениями о текущем состоянии или предлагает выполнить определенные действия. Если никакие сообщения не отображаются, это означает, что ваш компьютер защищен.

При необходимости можно в любой момент открыть окно Norton, чтобы просмотреть сводки о состоянии компьютера или подробные сведения о защите.

Norton уведомляет о выполняющейся в фоновом режиме операции при помощи сообщения в области уведомлений, находящейся в крайней правой части панели задач. Результаты последних операций можно просмотреть в главном окне Norton.

Включение и выключение автоматических задач

- 1 Запустите Norton.
Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.
- 2 В главном окне Norton щелкните **Параметры**.
- 3 В окне **Параметры** нажмите **Расписание задач**.

- 4 В окне **Расписание задач** откройте вкладку **Автоматические задачи** и выполните следующие действия.
 - Отметьте функции, которые должны выполняться автоматически. Включите переключатель **Задачи** для выбора всех функций.
 - Отмените выбор функций, которые не должны выполняться автоматически. Выключите переключатель **Задачи** для отмены выбора всех компонентов.
- 5 Нажмите кнопку **Применить**, а затем кнопку **Заккрыть**.

Выполнение пользовательских задач

Norton автоматически проверяет систему и выбирает оптимальные настройки для обеспечения ее безопасности. Однако можно выполнить некоторые специальные задачи. Для выполнения этих специальных задач можно использовать параметры, доступные в окне **Пользовательские задачи**.

Вы можете выбрать любое сочетание задач для однократного выполнения сканирования. Пользователь может выполнить LiveUpdate, создать резервную копию данных, очистить историю браузера, освободить место на диске за счет удаления ненужных файлов и оптимизировать диски.

Выполнение пользовательских задач

- 1 Запустите Norton.
 - Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.
- 2 В главном окне Norton дважды щелкните **Безопасность**, а затем выберите **Сканирования**.
- 3 В окне **Операции сканирования** в разделе **Сканирования и задачи** щелкните **Пользовательская задача**, а затем щелкните **Перейти**.
- 4 В окне **Пользовательские задачи** выберите задачи, которые необходимо выполнить. Чтобы выбрать все задачи, выберите **Задачи**.
- 5 Нажмите кнопку **Перейти**.

Планирование операций сканирования проблем безопасности и быстрого действия

Параметры расписания задач позволяют настроить в Norton автоматическую проверку безопасности и быстрого действия системы. Дополнительно можно указать, когда и как часто Norton должен выполнять такие проверки.

Предусмотрены следующие варианты расписания сканирования безопасности и быстрогодействия:

Автоматический (рекомендуется)	<p>Программа проверяет безопасность и быстродействие компьютера, когда он не используется.</p> <p>Этот вариант обеспечивает максимально надежную защиту.</p>
Еженедельно	<p>Программа проверяет безопасность и быстродействие компьютера один или несколько раз в неделю.</p> <p>Вы можете выбрать дни недели и время выполнения проверки.</p>
Ежемесячно	<p>Программа проверяет безопасность и быстродействие компьютера один раз в месяц.</p> <p>Вы можете выбрать число месяца и время выполнения проверки.</p>
Планирование вручную	<p>Не выполнять плановое сканирование безопасности и быстрогодействия компьютера.</p> <p>Если будет выбран этот вариант, то для обеспечения защиты компьютера вам потребуется вручную регулярно запускать сканирование безопасности и быстрогодействия.</p>

Планирование выполнения критических операций на время простоя компьютера позволяет сохранить максимальный уровень быстрогодействия. Если настроено еженедельное или ежемесячное сканирование и выбран параметр **Запускать только при простое**, то Norton будет выполнять сканирование компьютера только во время простоя. NortonLifeLock рекомендует выбирать параметр **Запускать только во время простоя** для повышения быстрогодействия компьютера.

Планирование операций сканирования проблем безопасности и быстрогодействия

- 1 Запустите Norton.
 Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.
- 2 В главном окне Norton щелкните **Параметры**.
- 3 В окне **Параметры** нажмите **Расписание задач**.

- 4 Выберите параметр на вкладке **Планирование** в разделе **Расписание**.

Для вариантов **Еженедельно** и **Ежемесячно** следует выбрать день и время выполнения автоматических задач. Кроме того, можно разрешить выполнение автоматических задач только во время простоя компьютера.

- 5 Нажмите кнопку **Применить**, а затем — кнопку **Заккрыть**.

Настройте Защитник данных для блокировки вредоносных процессов, оказывающих угрозу вашему компьютеру

Защитник данных защищает ваш компьютер от вредоносных процессов, мешающих работе и ставящих под угрозу ваши данные. При этом используется технология Norton для оценки процесса как безопасного, вредоносного или неизвестного. В зависимости от вашей ситуации, вы можете добавить больше папок и/или расширений или же отменить сканирование и защиту для определенных процессов.

Предупреждение! Отключение данной функции снижает степень защиты ПК. В связи с этим мы рекомендуем всегда оставлять данную функцию включенной. Если вы все же хотите отключить ее, делайте это лишь временно и после этого обязательно проверяйте, включилась ли она снова.

Включение и выключение защитника данных

- 1 Запустите Norton.

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

- 2 В главном окне продукта Norton щелкните **Параметры > Антивирус**.
- 3 В окне **Антивирус** выберите вкладку **Защитник данных**.
- 4 В строке **Защитник данных** переместите переключатель **Вкл./Выкл.** в положение **Выкл.** или **Вкл.**
- 5 В строке **Показать уведомления** выполните одно из следующих действий:
 - Для получения уведомлений обо всех угрозах, блокируемых Защитником данных, переместите переключатель в положение **Вкл.**
 - Для выключения уведомлений переместите переключатель в положение **Выкл.** Сведения о заблокированных угрозах можно просмотреть в окне **Журнал безопасности**.
Для того, чтобы открыть **Журнал безопасности**, перейдите в главное окно Norton, дважды щелкните значок **Безопасность** и выберите **Журнал > Защитник данных**.

- 6 Нажмите кнопку **Применить**.
- 7 Если появится соответствующий запрос, введите продолжительность периода, в течение которого компонент LiveUpdate должен быть выключен, а затем нажмите кнопку **ОК**.

Добавление или изменение папки для защитника данных

- 1 Запустите Norton.
Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.
- 2 В главном окне продукта Norton щелкните **Параметры > Антивирус**.
- 3 В окне **Антивирус** выберите вкладку **Защитник данных**.
- 4 В строке **Защитник данных** переместите переключатель **Вкл./Выкл.** в положение **Вкл.**
- 5 Чтобы добавить или изменить папку, выполните следующие действия:
 - Рядом со значком **Защищенные папки** нажмите **Настроить**.
 - Выполните следующие действия в окне **Защищенные папки** :
 - Чтобы добавить новый элемент, нажмите **Добавить**.
 - Чтобы изменить существующий элемент, выберите его, а затем нажмите кнопку **Изменить**.

Примечание: Редактировать предустановленную папку нельзя.

- В окне **Добавить элемент** или **Изменить элемент** найдите и выберите папку.
 - Установите флажок, чтобы добавить подпапки.
 - Нажмите кнопку **ОК**.
- 6 Нажмите кнопку **Применить**, а затем нажмите кнопку **ОК**.

Добавление расширения для защитника данных

- 1 Запустите Norton.
Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.
- 2 В главном окне продукта Norton щелкните **Параметры > Антивирус**.
- 3 В окне **Антивирус** выберите вкладку **Защитник данных**.
- 4 В строке **Защитник данных** переместите переключатель **Вкл./Выкл.** в положение **Вкл.**

- 5 Чтобы добавить расширение, сделайте следующее:
 - Рядом со значком **Защищенные типы файлов** нажмите **Настроить**.
 - В окне **Защищенные типы файлов** нажмите **Добавить**.
 - В окне **Добавить элемент** введите расширения, которое требуется добавить. Например, если вы хотите защитить открытые файлы, введите .exe. Все файлы с расширением .exe на ПК будут защищены.
 - Нажмите кнопку **ОК**.
- 6 Нажмите кнопку **Применить**, а затем нажмите кнопку **ОК**.

Удаление папки или расширения из защитника данных

- 1 Запустите Norton.

Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.
- 2 В главном окне продукта Norton щелкните **Параметры > Антивирус**.
- 3 В окне **Антивирус** выберите вкладку **Защитник данных**.
- 4 В строке **Защитник данных** переместите переключатель **Вкл./Выкл.** в положение **Вкл.**
- 5 Рядом со значком **Защищенные папки** или **Защищенные типы файлов** нажмите **Настроить**.
- 6 В окне **Защищенные папки** или **Защищенные типы файлов** выберите элемент, который требуется удалить.

Примечание: Удалить предустановленную папку или расширение нельзя.

- 7 Нажмите **Remove** (Удалить).
- 8 Нажмите кнопку **Применить**, а затем нажмите кнопку **ОК**.

Добавление или удаление процесса из защитника данных

- 1 Запустите Norton.

Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.
- 2 В главном окне продукта Norton щелкните **Параметры > Антивирус**.
- 3 В окне **Антивирус** выберите вкладку **Защитник данных**.
- 4 В строке **Защитник данных** переместите переключатель **Вкл./Выкл.** в положение **Вкл.**

- 5 В строке **Исключение процесса** нажмите **Настройка** и выполните следующие действия:
 - Чтобы исключить процесс, нажмите **Добавить**, а затем выберите процесс.
 - Чтобы отменить исключение процесса, необходимо выбрать его и нажать кнопку **Удалить**.
- 6 Нажмите кнопку **Применить**, а затем нажмите кнопку **ОК**.

Настройка Norton для удаления сценариев, которые могут быть использованы при попытках фишинга

Управление сценариями помогает обеспечить защиту от вредоносных программ, загружаемых или получаемых в виде вложений в фишинговых сообщениях электронной почты. Управление сценариями удаляет нестандартные сценарии из файлов и обрабатывает файлы по умолчанию**. Однако вы можете восстановить исходные файлы с помощью сценария и настроить, как Norton должен обрабатывать документы со встроенными сценариями.

Примечание: **Для браузеров Chrome, Edge и Internet Explorer параметр "Удалять сценарии при загрузке документов" доступен только в Windows 10 RS2 и более поздних версиях.

Кроме того, Norton блокирует программы со встроенными сценариями, если обнаруживает нестандартное поведение со встроенными сценариями. Однако вы можете настроить то, как Norton должен работать с программами со встроенными сценариями.

Сценарии используются, чтобы сделать документы динамическими и интерактивными. Хотя основная цель сценариев заключается в оптимизации работы с документами, киберпреступники могут использовать их для установки вредоносных программ на ваш компьютер. Обычно сценарии не важны для работы документа, и многие программы отключают их по умолчанию.

Можно настроить Norton таким образом, чтобы из управления сценариями исключались определенные файлы, если вы уверены, что они не содержат вредоносного содержимого. Для получения дополнительных сведений, см. статью См. ["Исключение файлов и папок из сканирований автоматической защиты Norton, SONAR и контроля загрузок"](#) на стр. 44. Исходные файлы можно восстановить, заменив обработанные файлы. Файлы следует исключать, только если вы уверены, что они не содержат вредоносных элементов.

Управление сценариями распознает потенциальные угрозы, исходя из поведения файлов. Если Norton обнаруживает какие-либо потенциально опасные действия при открытии документа или программы со встроенным сценарием, он блокирует приложение от

запуска сценария. Вы можете настроить то, как Norton должен обрабатывать сценарии при открытии документов или программ со встроенными сценариями.

Восстановление исходного файла

- 1 Запустите Norton.
Если отображается окно **Мой Norton** в строке **Безопасность устройства** нажмите **Открыть**.
- 2 В главном окне Norton дважды щелкните **Безопасность**, а затем выберите **Журнал**.
- 3 В окне **Журнал безопасности** в списке **Показать** выберите пункт **Управление сценариями**.
- 4 В представлении **Управление сценариями** выберите объект для восстановления.
- 5 На правой панели в разделе **Сведения** нажмите **Восстановить**.
- 6 В окне **Восстановление управления сценариями** нажмите **Да**.
- 7 В появившемся запросе подтверждения выберите **Да**.
- 8 В окне **Журнал безопасности** выберите **Заккрыть**.

Включение и выключение управления сценариями

- 1 Запустите Norton.
Если отображается окно **Мой Norton** в строке **Безопасность устройства** нажмите **Открыть**.
- 2 В главном окне Norton щелкните **Параметры**.
- 3 В окне **Параметры** выберите **Защита от вирусов**.
- 4 В окне параметров **Защита от вирусов** перейдите на вкладку **Управление сценариями**.
- 5 В строке **Удалять сценарии при загрузке документов** переместите переключатель **Вкл./Выкл.** в положение **Вкл.** или **Выкл.**, затем нажмите **Применить**.
В случае выключения выполните следующие действия:
 - В окне **Запрос безопасности** в раскрывающемся списке **Выберите продолжительность** укажите время, на которое необходимо отключить этот параметр, затем нажмите **ОК**.
- 6 В строке **Блокировка сценариев при открытии документов** переместите переключатель **Вкл./Выкл.** в положение **Выкл.** или **Вкл.**, затем нажмите **Применить**.
В случае выключения выполните следующие действия:

- В окне **Запрос безопасности** в раскрывающемся списке **Выберите продолжительность** укажите время, на которое необходимо отключить этот параметр, затем нажмите **ОК**.

7 В окне **Параметры** нажмите кнопку **Заккрыть**.

Удаление всех элементов управления сценариями без возможности восстановления

1 Запустите Norton.

Если отображается окно **Мой Norton** в строке **Безопасность устройства** нажмите **Открыть**.

2 В главном окне Norton щелкните **Параметры**.

3 В окне **Журнал безопасности** в списке **Показать** выберите пункт **Управление сценариями**.

4 В представлении **Управление сценариями** нажмите **Очистить записи**.

5 В окне **Очистить записи** нажмите **Да**.

6 В окне подтверждения нажмите кнопку **Да**.

7 В окне **Журнал безопасности** выберите **Заккрыть**.

Настройка того, как Norton должен обрабатывать документы или программы со встроенным сценарием

1 Запустите Norton.

Если отображается окно **Мой Norton** в строке **Безопасность устройства** нажмите **Открыть**.

2 В главном окне Norton щелкните **Параметры**.

3 В окне **Параметры** выберите **Защита от вирусов**.

4 В окне параметров **Защита от вирусов** перейдите на вкладку **Управление сценариями**.

5 В строке **Microsoft Office** под функцией **Блокировка сценариев при открытии документов** нажмите **Настроить**.

6 В окне **Настройки Microsoft Office** в списке **действий**, выберите действие, которое Norton должен выполнить для каждого приложения.

Предусмотрены следующие параметры:

- **Блокировать**
- **Разрешить**
- **Спросить меня**

Вы можете выбрать разное действие для каждого приложения.

- 7 В появившемся окне подтверждения нажмите **ОК**.
- 8 В окне **Настройки Microsoft Office** нажмите кнопку **Применить**, а затем — **ОК**.
- 9 В строке **Документ Adobe** выберите действие, которое Norton должен выполнять для документов PDF.
- 10 В строке **Блокировать сценарии с нестандартным поведением** выберите действие, которое Norton должен выполнять для программ со встроенными сценариями.
Предусмотрены следующие параметры:
 - **Блокировать**
 - **Разрешить**
 - **Спросить меня**
- 11 В окне **Параметры** нажмите кнопку **Применить**, а затем — кнопку **Заккрыть**.

Узнайте больше об Управлении сценариями Norton

Сценарии используются, чтобы сделать документы динамическими и интерактивными. Они также могут расширить функциональные возможности, автоматизируя определенные задачи. Сценарии могут включать элементы управления ActiveX, надстройки, соединения для передачи данных, макросы, связанные с объектами файлы, встроенные файлы OLE, файлы цветowych тем и т. д.

"Управление сценариями" помогает защитить вас от вредоносных программ, которые вы загружаете или получаете в виде вложений в фишинговых сообщениях эл. почты.

"Управление сценариями" удаляет небезопасные сценарии из файлов и обрабатывает файлы по умолчанию. Однако вы можете восстановить исходные файлы с помощью сценария и настроить, как Norton должен обрабатывать документы со встроенными сценариями.

Следующие разделы помогут вам настроить параметры "Управления сценариями".

Восстановление исходного файла со встроенными сценариями

Исходные файлы можно восстановить, заменив обработанные файлы. Исходные файлы следует восстанавливать, только если вы уверены, что они не содержат вредоносных элементов.

- 1 Запустите Norton.
Если отображается окно **Мой Norton** в строке **Безопасность устройства** нажмите **Открыть**.
- 2 В главном окне Norton дважды щелкните **Безопасность**, а затем выберите **Журнал**.
- 3 В окне **Журнал безопасности** в списке **Показать** выберите пункт **Управление сценариями**.
- 4 В представлении **Управление сценариями** выберите элемент активного содержимого для восстановления.
- 5 На правой панели в разделе **Сведения** нажмите **Восстановить**.
- 6 В окне **Восстановление управления сценариями** нажмите **Да**.
- 7 В появившемся запросе подтверждения выберите **Да**.
- 8 В окне **Журнал безопасности** выберите **Заккрыть**.

Настройка Norton для обработки документов и программ со встроенным сценарием

- 1 Запустите Norton.
Если отображается окно **Мой Norton** в строке **Безопасность устройства** нажмите **Открыть**.
- 2 В главном окне Norton щелкните **Параметры**.
- 3 В окне **Параметры** выберите **Защита от вирусов**.
- 4 В окне параметров **Защита от вирусов** перейдите на вкладку **Управление сценариями**.
- 5 В строке **Microsoft Office** под функцией **Блокировка сценариев при открытии документов** нажмите **Настроить**.
- 6 В окне **Настройки Microsoft Office** в списке **действий**, выберите действие, которое Norton должен выполнить для каждого приложения.
Предусмотрены следующие параметры:
 - **Блокировать**
 - **Разрешить**
 - **Спросить меня**Вы можете выбрать разное действие для каждого приложения.
- 7 В появившемся окне подтверждения нажмите **ОК**.
- 8 В окне **Настройки Microsoft Office** нажмите кнопку **Применить**, а затем — **ОК**.

- 9 В строке **Документ Adobe** выберите действие, которое Norton должен выполнять для документов PDF.
- 10 В строке **Блокировать сценарии с нестандартным поведением** выберите действие, которое Norton должен выполнять для программ со встроенными сценариями.

Предусмотрены следующие параметры:

- **Блокировать**
- **Разрешить**
- **Спросить меня**

- 11 В окне **Параметры** нажмите кнопку **Применить**, а затем кнопку **Заккрыть**.

Отключение управления сценариями

Примечание: Отключение управления сценариями ослабляет защиту и должно применяться только в случае крайней необходимости. Управление сценариями обеспечивает дополнительную безопасность путем удаления сценариев и очистки документов. NortonLifeLock рекомендует всегда оставлять параметр управления сценариями включенным, поскольку это обеспечивает дополнительный уровень безопасности.

- 1 Запустите Norton.
Если отображается окно **Мой Norton** в строке **Безопасность устройства** нажмите **Открыть**.
- 2 В главном окне Norton щелкните **Параметры**.
- 3 В окне **Параметры** выберите **Защита от вирусов**.
- 4 В окне параметров **Защита от вирусов** перейдите на вкладку **Управление сценариями**.
- 5 В строке **Удалять сценарии при загрузке документов** переместите переключатель **Вкл./Выкл.** в положение **Выкл.**.
- 6 В строке **Блокировка сценариев при открытии документов** переместите переключатель **Вкл./Выкл.** в положение **Выкл.**.
- 7 В окне **Параметры** нажмите кнопку **Применить**.

- 8 В окне **Запрос безопасности** в раскрывающемся списке **Выберите продолжительность** укажите время, на которое необходимо отключить данную опцию, затем нажмите **ОК**.
- 9 В окне **Параметры** нажмите кнопку **Заккрыть**.

Защитите свое устройство от эксплойтов, хакеров и атак нулевого дня

Эксплойт нулевого дня — это метод, применяемый хакерами для использования уязвимостей в программе для выполнения вредоносных действий на компьютере. Помимо замедления работы компьютера и нарушения работы программ, эти эксплойты могут передавать вашу личную и конфиденциальную информацию хакерам.

Компонент предотвращения использования эксплойтов в установленном продукте Norton защищает приложения и файлы, являющиеся привлекательной мишенью для атак. По умолчанию компонент предотвращения использования эксплойтов Norton включен и блокирует атаки, закрывая уязвимые программы, на которые направлены эти атаки. Norton отправляет уведомление "Атака заблокирована", когда выключает программу, и предоставляет ссылки на информацию об атаке.

Включение и выключение компонента предотвращения использования эксплойтов

Примечание: Когда **Предотвращение использования эксплойтов** выключено, ваш компьютер уязвим для эксплойтов нулевого дня и других типов эксплойтов.

- 1 Запустите Norton.
Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.
- 2 В главном окне Norton щелкните **Параметры**.
- 3 В окне Параметры нажмите **Предотвращение использования эксплойтов**.
- 4 В строке Предотвращение использования эксплойтов переместите переключатель **Вкл./Выкл.** в положение **Выкл.** или **Вкл.**
- 5 В окне Параметры нажмите кнопку **Применить**, а затем кнопку **Заккрыть**.

Методы предотвращения использования эксплойтов

Norton использует превентивное предотвращение использования эксплойтов для защиты компьютера от новейших атак нулевого дня. Вы можете включить или выключить отдельные методы в окне **Параметры**. По умолчанию включены все методы.

Примечание: Norton рекомендует оставить все отдельные методы предотвращения использования эксплойтов включенными, чтобы обеспечить максимально возможную защиту.

К методам предотвращения использования эксплойтов относятся:

- **Защита Java-процессов**

Предотвращает применение вредоносного кода через Java-процессы со стороны удаленных хакеров и позволяет запускать только надежные Java-процессы.

- **Защита от перезаписи структурированного обработчика исключений**

Защищает от эксплойтов структурированного обработчика исключений, которые ставят под угрозу приложение, перезаписывая указатель обработчика исключений адресом, который контролирует злоумышленник.

- **Обнаружение сводных данных стека**

Блокирует атаки с использованием эксплойтов, которые изменяют указатель стека с помощью управляемой памяти злоумышленника для выполнения вредоносного кода возвратно-ориентированного программирования.

- **Принудительное предотвращение выполнения данных**

Не дает злоумышленникам выполнять вредоносный код из стека или динамической памяти вашего компьютера.

- **Принудительная случайная выборка структуры памяти**

Обеспечивает загрузку динамически загружаемых библиотек DLL или модулей в случайные расположения, чтобы защитить их от злоумышленников.

- **Защита распределения кучи**

Защищает часто атакуемые адреса памяти, в которых эксплойты или злоумышленники размещают свой шелл-код с использованием методов атаки распределения кучи.

- **Улучшение случайной выборки структуры памяти**

Улучшает поведение ASLR (случайного распределения адресного пространства) операционной системы при распределении критических важных адресов памяти приложения. Это делает такие адреса памяти менее предсказуемыми для злоумышленников.

- **Защита страницы NULL**

Предварительно распределяет нулевой адрес памяти, что может помочь предотвратить атаки с использованием уязвимостей, вызывающих разыменование нулевого указателя.

- **Обнаружение удаленного внедрения DLL**

Не дает удаленным хакерам добавлять вредоносный исполняемый код через внешние сети, такие как общедоступные IP-адреса или домены.

- Методы **Предотвращение выполнения стека**, **Обнаружение подозрительного вызова API** и **Обнаружение полезной нагрузки кучи** защищают компьютер от атак с использованием возвратно-ориентированного программирования (ROP), которые обходят методы случайного распределения адресного пространства и предотвращения выполнения данных.

Включение и выключение брандмауэра Norton

Интеллектуальный брандмауэр отслеживает все соединения вашего компьютера с другими компьютерами сети Интернет. Он также защищает компьютер от наиболее распространенных проблем безопасности. Когда интеллектуальный брандмауэр выключен, компьютер не защищен от угроз, связанных с работой в Интернете.

Интеллектуальный брандмауэр можно отключить только на определенный период времени, по истечении которого он будет включен автоматически.

Включение и выключение брандмауэра Norton

- 1 Запустите Norton.
Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.
- 2 В главном окне Norton щелкните **Параметры**.
- 3 В окне **Параметры** нажмите **Брандмауэр**.
- 4 На вкладке **Общие параметры** в строке **Интеллектуальный брандмауэр** переместите переключатель **Вкл./Выкл.** в положение **Выкл.** или **Вкл.**
- 5 Нажмите кнопку **Применить**.
- 6 Если появится соответствующий запрос, введите продолжительность периода, в течение которого брандмауэр должен быть выключен, а затем нажмите кнопку **ОК**.

Включение и выключение брандмауэра Norton в области уведомлений Windows

- 1 В области уведомлений на панели задач щелкните правой кнопкой значок Norton и выберите **Выключить интеллектуальный брандмауэр** или **Включить интеллектуальный брандмауэр**.
- 2 Если появится соответствующий запрос, введите продолжительность периода, в течение которого брандмауэр должен быть выключен, а затем нажмите кнопку **ОК**.

Настройка правил программы для изменения параметров доступа для программ

В процессе работы с Norton может потребоваться изменить параметры доступа для некоторых программ.

Настройка правил для программ

- 1 Запустите Norton.

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

- 2 В главном окне Norton щелкните **Параметры**.
- 3 В окне **Параметры** нажмите **Брандмауэр**.
- 4 На вкладке **Управление программами** в столбце **Программа** выберите программу, которую требуется изменить.
- 5 В показанном рядом с программой раскрывающемся списке выберите необходимый уровень доступа. Предусмотрены следующие параметры.

Разрешить	Разрешает программе все виды доступа.
Блокировать	Запрещает программе все виды доступа.
Настраиваемое	Позволяет создать правила, управляющие доступом программы к сети Интернет.

- 6 Нажмите кнопку **Применить**.

Изменение порядка обработки правил брандмауэра

Списки правил брандмауэра обрабатываются сверху вниз. Для изменения порядка обработки правил измените их расположение в списке.

Примечание: Не изменяйте порядок стандартных правил обработки трафика, если у вас нет достаточного опыта работы с продуктом. Изменение порядка этих правил может повлиять на работу брандмауэра и ослабить защиту компьютера.

Изменение порядка правил обработки трафика

- 1 Запустите Norton.
Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.
- 2 В главном окне Norton щелкните **Параметры**.
- 3 В окне **Параметры** нажмите **Брандмауэр**.
- 4 На вкладке **Правила трафика** выберите правило для перемещения.
- 5 Выполните одно из следующих действий:

- Для того чтобы переместить выбранное правило выше по списку, нажмите кнопку **Вверх**.
 - Для того чтобы переместить выбранное правило ниже по списку, нажмите кнопку **Вниз**.
- 6 После перемещения всех необходимых правил нажмите кнопку **Применить**.

Изменение порядка обработки правил программ

- 1 Запустите Norton.
Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.
- 2 В главном окне Norton щелкните **Параметры**.
- 3 В окне **Параметры** нажмите **Брандмауэр**.
- 4 На вкладке **Управление программами** выберите программу, содержащую правило, которое требуется переместить.
- 5 Нажмите кнопку **Изменить**.
- 6 В окне **Правила** выберите правило для перемещения.
- 7 Выполните одно из следующих действий:
 - Для того чтобы переместить выбранное правило выше по списку, нажмите кнопку **Вверх**.
 - Для того чтобы переместить выбранное правило ниже по списку, нажмите кнопку **Вниз**.
- 8 После перемещения всех необходимых правил нажмите кнопку **ОК**.
- 9 В окне **Брандмауэр** нажмите кнопку **Применить**.

Временное отключение правила обработки трафика

Правило обработки трафика можно на время выключить, чтобы разрешить определенный вид доступа к компьютеру или программе. Не забудьте снова включить правило, когда выполните в программе или на компьютере операцию, для которой потребовалось внести это изменение.

Примечание: Список содержит ряд правил по умолчанию, которые невозможно выключить. Однако их можно просмотреть с помощью функции **Показать**.

Временное отключение правила обработки трафика

- 1 Запустите Norton.
Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.
- 2 В главном окне Norton щелкните **Параметры**.
- 3 В окне **Параметры** нажмите **Брандмауэр**.
- 4 На вкладке **Правила трафика** снимите флажок рядом с правилом, которое необходимо выключить.
- 5 Нажмите кнопку **Применить**.

Разрешить доступ к Интернету для заблокированной программы

По умолчанию интеллектуальный брандмауэр блокирует некоторым программам доступ к Интернету. Такие программы могут включать в себя программы обработки потокового аудио- и видео, сетевые игры или нестандартные деловые приложения, применяемые внутри организации. Если вы знаете, что доступ программы к Интернету не несет угрозы безопасности компьютера, то разблокируйте его.

Разрешить доступ к Интернету для заблокированной программы

- 1 Запустите Norton.
Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.
- 2 В главном окне Norton щелкните **Параметры**.
- 3 В окне **Параметры** нажмите **Брандмауэр**.
- 4 На вкладке **Управление программами** выберите программу, которой необходимо разрешить доступ в Интернет.
- 5 В поле **Доступ** рядом с программой выберите значение **Разрешить**.
- 6 Нажмите кнопку **Применить**.

По умолчанию брандмауэр Norton автоматически настраивает параметры доступа к Интернету при первом запуске программ, использующих подключение к Интернету. Когда программа впервые пытается подключиться к Интернету, функция автоматического управления программами создает для нее правила.

Однако Norton позволяет вам вручную настроить параметры доступа к Интернету для ваших программ.

Как настроить параметры доступа к Интернету для программ

Выключение автоматического управления программами

- 1 Запустите Norton.
Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.
- 2 В главном окне Norton щелкните **Параметры**.
- 3 В окне **Параметры** нажмите **Брандмауэр**.
- 4 В окне параметров **Брандмауэр** щелкните **Расширенное управление программами**.
- 5 В строке **Расширенное управление программами** переместите переключатель **Вкл./Выкл.** в положение **Выкл.**
- 6 В окне подтверждения нажмите кнопку **Да**.
- 7 В окне **Параметры** нажмите кнопку **Применить**, а затем кнопку **Заккрыть**.

Как настроить параметры доступа к Интернету для программы

- 1 Запустите программу.
Когда программа пытается получить доступ к Интернету, Norton отправляет предупреждение брандмауэра.
- 2 В окне **Предупреждение брандмауэра** в раскрывающемся списке **Параметры** выберите действие.
Мы можете разрешить, заблокировать или вручную создать правило программы.
- 3 Нажмите кнопку **ОК**.

Выключение уведомления о блокировании брандмауэром

Если включено автоматическое управление программами, интеллектуальный брандмауэр автоматически блокирует попытки вредоносных приложений и приложений с низкой репутацией подключиться к Интернет или другим устройствам в сети.

Norton уведомляет о блокировке интеллектуальным брандмауэром подключения приложения к сети. Чтобы это уведомление не отображалось, его можно отключить с помощью **Расширенного управления программами**.

Выключение уведомления о блокировании брандмауэром

- 1 Запустите Norton.
Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.
- 2 В главном окне Norton щелкните **Параметры**.

- 3 В окне **Параметры** нажмите **Брандмауэр**.
- 4 На вкладке **Расширенное управление программами** переместите переключатель **Показывать уведомление о блокировке брандмауэром** в положение **Выкл.**

Подробнее о списке исключений системы предотвращения вторжений

Для безопасных устройств в сети можно указать уровень надежности "Полная надежность". Можно настроить уровень надежности устройства с помощью параметра "Надежность устройства" в разделе **Настройки сети**. Надежные устройства можно исключить из сканирования системы предотвращения вторжений. Путем исключения устройств с полной надежностью из сканирования системы предотвращения вторжений можно сократить время сканирования и повысить быстродействие сети. При исключении устройства с полной надежностью продукт Norton не сканирует информацию, получаемую из этого устройства. Устройства с полной надежностью, исключенные из сканирования системы предотвращения вторжений, добавляются в список исключений системы предотвращения вторжений.

В случае заражения устройств, исключенных из сканирования системы предотвращения вторжений, рекомендуется очистить сохраненный список исключений. При очистке списка исключений продукт Norton удаляет из него все устройства, которые ранее были исключены из операций сканирования, осуществляемых системой предотвращения вторжений.

Сохраненный список исключений рекомендуется очищать в следующих случаях:

- Заражение устройства, исключенного из сканирования системы предотвращения вторжений.
- Попытка заражения компьютера устройством, исключенным из сканирования системы предотвращения вторжений.
- Заражение домашней сети.

Удаление всех устройств из списка исключений системы предотвращения вторжений

- 1 Запустите Norton.
Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.
- 2 В главном окне Norton щелкните **Параметры**.
- 3 В окне **Параметры** нажмите **Брандмауэр**.
- 4 Откройте вкладку **Вторжения и защита браузера**.
- 5 В разделе **Предотвращение вторжений** в строке **Список исключений** выберите **Очистить**.

- 6 В окне подтверждения нажмите кнопку **Да**.
- 7 В окне **Параметры** нажмите кнопку **Заккрыть**.

Включение защиты веб-браузера

Вредоносные веб-сайты способны обнаруживать и использовать уязвимости браузеров для загрузки вредоносных программ. При включенной функции защиты веб-браузера Norton блокирует вредоносные программы еще до начала атаки. Она обеспечивает безопасность конфиденциальной информации и не позволяет атакующим получить доступ к компьютеру.

По умолчанию функция "Защита веб-браузера" включена. Рекомендуем никогда не выключать функцию "Защита веб-браузера", чтобы обеспечить защиту от атак с вредоносных веб-сайтов.

Примечание: Компонент защиты веб-браузера доступен для браузеров Google Chrome, Microsoft Internet Explorer, Mozilla Firefox и Microsoft Edge.

Как включить функцию защиты веб-браузера?

Функция защиты веб-браузера включена по умолчанию, чтобы браузер был защищен от атак с вредоносных веб-сайтов. Если она по каким-либо причинам была выключена, то ее можно включить обратно.

Включение защиты веб-браузера

- 1 Запустите Norton.
Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.
- 2 В главном окне продукта Norton щелкните **Параметры**.
- 3 В окне Параметры нажмите **Брандмауэр** или **Сеть**.
- 4 Откройте вкладку **Вторжения и защита браузера**.
- 5 В строке "Защита веб-браузера" переместите переключатель **Вкл./Выкл.** в положение **Вкл.**

- 6 Нажмите кнопку **Применить**.
- 7 В окне **Параметры** нажмите кнопку **Заккрыть**.

Настройка брандмауэра Norton для включения или выключения уведомлений о блокировании атак

Укажите, следует ли системе предотвращения вторжений Norton показывать уведомления о блокировании потенциальных атак.

Если вы не получаете уведомления, заблокированные Norton атаки можно просмотреть в журнале безопасности.

Включение и выключение уведомлений системы предотвращения вторжений

- 1 Запустите Norton.
Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.
- 2 В главном окне Norton щелкните **Параметры**.
- 3 В окне **Параметры** нажмите **Брандмауэр** или **Сеть**.
- 4 Откройте вкладку **Вторжения и защита браузера**.
- 5 В разделе **Предотвращение вторжений** в строке **Уведомления** переместите переключатель **Вкл./Выкл.** в положение **Выкл.** или **Вкл.**
- 6 В окне **Параметры** нажмите кнопку **Применить**, а затем нажмите кнопку **Заккрыть**.

Включение и выключение отдельного уведомления системы предотвращения вторжений

- 1 Запустите Norton.
Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.
- 2 В главном окне Norton щелкните **Параметры**.
- 3 В окне **Параметры** нажмите **Брандмауэр** или **Сеть**.
- 4 Откройте вкладку **Вторжения и защита браузера**.
- 5 В разделе **Предотвращение вторжений** в строке **Сигнатуры вторжений** нажмите кнопку **Настроить**.
- 6 В окне **Сигнатуры вторжений** установите или снимите флажок **Уведомлять меня** в зависимости от используемой сигнатуры.
- 7 Нажмите кнопку **ОК**.
- 8 В окне **Сигнатуры вторжений** нажмите кнопку **Применить** и затем кнопку **ОК**.
- 9 В окне **Параметры** нажмите кнопку **Заккрыть**.

Включение и выключение функции автоматической блокировки

Автоматическая блокировка Norton прерывает обмен данными между устройством в вашей сети и любым другим компьютером, который пытается воспользоваться уязвимостью этого устройства. Так как сюда входит трафик, который может не быть вредоносным, автоматическая блокировка прерывает соединение на ограниченный период времени после обнаружения угрозы. Можно указать период времени, в течение которого продукт Norton будет блокировать соединения с атакующими компьютерами. По умолчанию продукт Norton блокирует весь трафик между компьютером пользователя и атакующим компьютером в течение 30 минут.

При необходимости функцию автоматической блокировки можно выключить, чтобы обратиться к заблокированным компьютерам.

Включение и выключение функции автоматической блокировки

- 1 Запустите Norton.
Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.
- 2 В главном окне Norton щелкните **Параметры**.
- 3 В окне **Параметры** нажмите **Брандмауэр** или **Сеть**.
- 4 Откройте вкладку **Вторжения и защита браузера**.
- 5 В разделе **Предотвращение вторжений** в строке **Автоматическая блокировка вторжений** нажмите кнопку **Настроить**.
- 6 В окне **Автоматическая блокировка вторжений** выполните одно из следующих действий в разделе **Автоматическая блокировка**.
 - Для выключения автоматической блокировки вторжений выберите **Выкл.**
 - Чтобы включить автоматическую блокировку вторжений, выберите **Включить (рекомендуется)**, а затем из раскрывающегося списка **Автоматическая блокировка атакующих компьютеров на** выберите время, в течение которого будет работать автоматическая блокировка.
- 7 В окне **Автоматическая блокировка вторжений** нажмите кнопку **ОК**.
- 8 В окне **Параметры** нажмите кнопку **Заккрыть**.

Разблокировка компьютеров, заблокированных функцией автоматической блокировки

Если брандмауэр Norton останавливает сетевой трафик с безопасным компьютером, вы можете восстановить соединение с этим компьютером, удалив его из списка автоматической блокировки в настройках брандмауэра Norton.

Разблокировка автоматически заблокированного компьютера

- 1 Запустите Norton.
Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.
- 2 В главном окне Norton щелкните **Параметры**.
- 3 В окне **Параметры** нажмите **Брандмауэр** или **Сеть**.
- 4 Откройте вкладку **Вторжения и защита браузера**.
- 5 В разделе **Предотвращение вторжений** в строке **Автоматическая блокировка вторжений** нажмите кнопку **Настроить**.
- 6 В окне **Автоматическая блокировка вторжений** в разделе **Компьютеры, заблокированные функцией автоматической блокировки** выберите IP-адрес компьютера.
- 7 В столбце **Действие** выберите в раскрывающемся списке пункт **Разблокировать**.
- 8 В окне "Автоматическая блокировка вторжений" нажмите кнопку **ОК**.
- 9 В окне **Параметры** нажмите кнопку **Заккрыть**.

Добавление устройства в список надежности устройств

Можно вручную добавить устройство в число надежных. Для добавления устройства необходимо указать следующие данные:

- Имя и описание устройства
- IP-адрес или физический адрес устройства

Примечание: Добавление в число надежных устройства из другой сети может поставить под угрозу безопасность компьютера.

Добавление устройства в список надежности устройств

- 1 Запустите Norton.
Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.
- 2 В главном окне Norton щелкните **Параметры**.
- 3 В окне **Параметры** нажмите **Брандмауэр**.
- 4 На вкладке **Общие параметры** в строке **Надежность устройства** щелкните **Настроить**.
- 5 В окне **Надежность устройства** щелкните **Добавить**.

- 6** В окне **Добавить устройство** в поле **Имя** введите имя устройства, добавляемого в сеть.

Длина имени устройства не должна превышать 15 символов.

- 7** В поле **IP-адрес или физический адрес** введите IP-адрес или физический адрес устройства, добавляемого в список надежности устройств.

Значение в поле **IP-адрес или физический адрес** должно быть задано в одном из следующих форматов:

Адрес IPv4	172.16.0.0
Адрес IPv6	fe80::12ac:fe44:192a:14cc
Физический адрес	11-22-c3-5a-fe-a4
Имя хоста	ftp.myfiles.com

Указанные адреса не проверяются до момента физического обнаружения устройства в сети.

- 8** Выберите нужный вариант из раскрывающегося меню **Уровень надежности**. Предусмотрены следующие параметры.

Полная надежность

Добавляет устройство в список устройств с полной надежностью.

На устройствах из группы с полной надежностью отслеживается только появление известных атак и способов заражения. Этот вариант следует выбирать только в том случае, если устройство полностью безопасно.

Запрещено

Добавляет устройство в список запрещенных.

Устройствам из списка запрещенных запрещен доступ к этому компьютеру.

- 9** Если необходимо исключить устройство из операций сканирования системы предотвращения вторжений, установите параметр **Исключить из сканирования IPS**.

- 10** Нажмите кнопку **Добавить устройство**.

Включение и выключение контроля загрузок

Download Insight защищает компьютер от вредоносных файлов, которые могут быть запущены после их загрузки с помощью поддерживаемого браузера. По умолчанию параметр **Контроль загрузок** включен. Download Insight предоставляет информацию об уровне репутации всех загружаемых исполняемых файлов. Сведения о репутации, предоставляемые функцией Download Insight, служат индикатором того, насколько безопасно устанавливать загруженный файл.

В некоторых случаях может потребоваться выключить функцию Download Insight. Например, если вам потребуется загрузить небезопасный файл. В этом случае необходимо отключить функцию Download Insight, чтобы продукт Norton позволил загрузить файл и не удалял его с компьютера.

Функцию Download Insight можно включить или выключить с помощью функции **Контроль загрузок**.

Включение и выключение функции Контроль загрузок

- 1 Запустите Norton.
 Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.
- 2 В главном окне продукта Norton щелкните **Параметры**.
- 3 В окне **Параметры** нажмите **Брандмауэр** или **Сеть**.
- 4 Откройте вкладку **Вторжения и защита браузера**.
- 5 В строке **Контроль загрузок** переместите переключатель **Вкл./Выкл.** в положение **Выкл.** или **Вкл.**
- 6 Нажмите кнопку **Применить**.
- 7 Если появится соответствующий запрос, введите продолжительность периода, в течение которого компонент Контроль загрузок должен быть выключен, а затем нажмите кнопку **ОК**.
- 8 В окне **Параметры** нажмите кнопку **Заккрыть**.

Включение и выключение функции фильтрации спама

С ростом популярности электронной почты увеличивается поток нежелательных коммерческих электронных сообщений, известных как спам, которые рассылаются пользователям без их разрешения. Среди спама трудно найти полезные электронные сообщения, а часть спама содержит текст и изображения сомнительного характера.

Для контроля за этими спам-сообщениями можно использовать функции фильтрации спама. По умолчанию защита от спама активна. При необходимости ее можно выключить в самой программе.

Примечание: Выключение компонента Norton AntiSpam повышает риск получения нежелательных сообщений электронной почты.

Включение и выключение функции фильтрации спама

- 1 Запустите Norton.
Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.
- 2 В главном окне продукта Norton щелкните **Параметры**.
- 3 В окне **Параметры** нажмите **Защита от спама**.
- 4 На вкладке **Фильтр** в строке **Защита от спама** переместите переключатель **Вкл./Выкл.** в положение **Выкл.** или **Вкл.**
- 5 После выключения интеллектуальной фильтрации спама выполните следующие действия:
 - В окне **Запрос безопасности** укажите время, на которое необходимо выключить фильтрацию спама, в раскрывающемся списке **Выберите продолжительность**.
- 6 Нажмите кнопку **Применить**.
- 7 Нажмите кнопку **ОК**.
- 8 В окне **Параметры** нажмите кнопку **Заккрыть**.

Ограничение использования Интернета для Norton

Функция **Ограничение использования сети** позволяет настроить пропускную способность, используемую Norton. По умолчанию параметр "Ограничение использования сети" имеет значение "Авто". В Windows 7 и более ранних версиях по умолчанию применяется параметр **Без ограничений**. При низкой скорости подключения к Интернет можно уменьшить используемую Norton пропускную способность. Также можно настроить политику передачи данных для всех сетевых соединений, используемых вашим компьютером, изменив настройки раздела "Ограничение использования сети".

Ограничение использования Интернета для Norton

- 1 Запустите Norton.
Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.
- 2 В главном окне Norton щелкните **Параметры**.
- 3 В окне **Параметры** нажмите **Брандмауэр**.

- 4 На вкладке **Общие параметры** в строке **Ограничение использован. сети** нажмите кнопку **Настроить**. Если параметр **Настроить** выключен, переместите переключатель **Вкл./Выкл.** в положение **Вкл.**
- 5 В окне настроек **Ограничение использован. сети** в столбце **Политика** щелкните раскрывающийся список рядом с сетевым соединением, для которого необходимо настроить политику.
- 6 Выберите один из следующих вариантов:
 - **Авто** : позволяет получать все обновления продукта и описания вирусов на основе политики осведомленности о стоимости Windows.

Примечание: Параметр Авто доступен только в Windows 8 и более новых версиях.

- **Без ограничений** : позволяет продукту Norton использовать пропускную способность сети, необходимую для получения всех обновлений продукта и описаний вирусов. При использовании Windows 7 или более ранней версии по умолчанию применяется политика **Без ограничений**.
 - **Экономия** : позволяет продукту Norton использовать Интернет только для получения критических обновлений продукта и описаний вирусов. Если пропускная способность подключения к Интернету ограничена, то выбор параметра **Экономия** позволит гарантировать защиту от самых опасных угроз.
 - **Нет трафика** : запрещает Norton доступ в Интернет. Если будет выбрана эта политика, Norton не сможет получать критические обновления программы и описания вирусов, что может привести к снижению уровня безопасности и уязвимости перед вирусными атаками.
- 7 Щелкните **Применить**, а затем — **ОК**.
 - 8 В окне **Параметры** нажмите кнопку **Заккрыть**.

Включение и выключение функции "Ограничение использования сети"

Чтобы ограничить использование Интернет программой Norton, можно настроить определенные политики. Если не требуется ограничивать использование Интернет продуктом Norton, функцию **Ограничение использования сети** можно отключить.

Если есть подозрение, что Norton использует слишком большую долю пропускной способности сети, можно включить функцию **Ограничение использования сети**. Затем можно настроить требуемые политики, чтобы ограничить использование Интернет со стороны Norton. Продукт Norton подключается к Интернет согласно политике, заданной

Настройте Norton, чтоб отслеживать приложения и запретить доступ к вашему компьютеру вредоносным веб-сайтам

в окне настроек **Ограничение использования сети**. По умолчанию **Ограничение использования сети** включен.

Включение и выключение функции "Ограничение использования сети"

- 1 Запустите Norton.
Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.
- 2 В главном окне Norton щелкните **Параметры**.
- 3 В окне **Параметры** нажмите **Брандмауэр**.
Если у вас есть Norton AntiVirus, нажмите **Сеть**.
- 4 На вкладке **Общие параметры** в строке **Ограничение использования сети** переместите переключатель **Вкл./Выкл.** в положение **Выкл.** или **Вкл.**
- 5 В окне **Параметры** нажмите кнопку **Применить**, а затем — кнопку **Заккрыть**.

Настройте Norton, чтоб отслеживать приложения и запретить доступ к вашему компьютеру 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 **Мониторинг URL-адреса приложения** включен, Norton будет отслеживать все приложения, установленные на вашем устройстве, а также блокировать доступ к вашему компьютеру вредоносным веб-сайтам. При блокировке вредоносного веб-сайта будет отправлено уведомление. Сведения об атаке можно просмотреть в журнале безопасности.

Примечание: Функция **Мониторинг URL-адреса приложения** не отслеживает приложения браузера. Для защиты приложений браузера от вредоносных веб-сайтов в браузер необходимо добавить расширения Norton.

Настройте Norton, чтоб отслеживать приложения и запретить доступ к вашему компьютеру вредоносным веб-сайтам

Включение функции «Мониторинг URL-адреса приложения» для блокировки вредоносных веб-сайтов

Функция **Мониторинг URL-адреса приложения** включена по умолчанию. Рекомендуем не отключать функцию «Мониторинг URL-адреса приложения», чтобы обеспечить защиту от атак с вредоносных веб-сайтов.

- 1 Запустите Norton.
Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.
- 2 В главном окне Norton щелкните **Параметры**.
- 3 В окне **Параметры** нажмите **Брандмауэр** или **Сеть**.
- 4 Откройте вкладку **Вторжения и защита браузера**.
- 5 В разделе **Предотвращение вторжений** в строке **Мониторинг URL-адреса приложения** переместите переключатель «Вкл./Выкл.» в положение «Вкл».

Исключение URL-адреса или домена из числа отслеживаемых

Для обнаружения и блокировки подозрительных веб-сайтов с помощью функции «предотвращение вторжений» 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 сигнатуры можно исключить из числа отслеживаемых.

Исключение URL-адреса или домена из уведомления о предупреждении

- 1 В уведомлении о предупреждении щелкните **Подробнее**.
- 2 В окне **Журнал безопасности — Дополнительные сведения** нажмите **Разблокировать URL**.

Исключение URL-адреса или домена с помощью Norton

- 1 Запустите Norton.
Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.
- 2 В главном окне Norton щелкните **Параметры**.
- 3 В окне **Параметры** нажмите **Брандмауэр** или **Сеть**.
- 4 Откройте вкладку **Вторжения и защита браузера**.
- 5 В разделе **Предотвращение вторжений** в строке **Исключения мониторинга URL-адреса приложения** нажмите **Настроить**.

- 6 Нажмите кнопку **Добавить** и введите URL-адрес или имя домена, которые необходимо исключить из числа отслеживаемых.
- 7 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.
 - Выберите URL-адрес или домен, который необходимо удалить, и нажмите кнопку **Удалить**.

Просмотр сведений о заблокированном URL-адресе

Просмотр сведений в уведомлении о предупреждении

- 1 В уведомлении о предупреждении щелкните **Подробнее**.
- 2 Сведения о заблокированном URL-адресе можно просмотреть в окне **Журнал безопасности — Дополнительные сведения**.

Просмотр информации в окне «Журнал безопасности»

- 1 Запустите Norton.
Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.
- 2 В главном окне продукта Norton дважды щелкните **Безопасность**, а затем выберите **Журнал**.
- 3 В окне **Журнал безопасности** в раскрывающемся списке **Показать** выберите пункт **Предотвращение вторжений**.
- 4 Для просмотра сведений об объекте выберите соответствующую строку.
- 5 Дважды щелкните строку или нажмите **Дополнительные настройки**, чтобы открыть «Журнал безопасности — Дополнительные сведения» и ознакомиться с более подробной информацией о действиях и, при необходимости, принять необходимые меры.

Начало использования резервного копирования в облаке Norton

Функция резервного копирования в облаке хранит и защищает важные файлы и документы, предотвращая потерю данных в связи с ошибками жесткого диска, кражей устройств и даже работой программ-вымогателей.

Примечание: Резервное копирование в облаке доступно только в операционных системах Windows.

Перед запуском резервного копирования Norton создайте набор данных резервного копирования с указанием файлов, для которых необходимо создать резервную копию. Также можно указать, где необходимо создавать резервные копии файлов и когда выполнять резервное копирование. Файлы резервной копии могут храниться в облачном хранилище Norton или на ваших собственных внешних дисках.

Примечание: Во время первого запуска резервного копирования программе Norton может потребоваться некоторое время на проверку и копирование всех файлов. При медленном соединении с Интернетом этот процесс может занять больше времени.

Norton не создает резервную копию файлов, если целевым расположением резервного копирования является локальное резервное копирование. Для создания резервных копий на локальном устройстве хранения необходимо вмешательство пользователя.

Создание набора данных резервного копирования

- 1 Запустите Norton.
Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.
- 2 В главном окне Norton дважды щелкните **Резервное копирование** и выберите **Наборы данных резервного копирования**.
- 3 В окне **Параметры резервного копирования** нажмите **Создать новый набор**.
- 4 В появившемся окне введите имя набора данных резервного копирования и затем нажмите **ОК**.
- 5 На вкладке **Что**, в разделе **Типы файлов**, включите одну или несколько категорий файлов, для которых необходимо создать резервную копию.
- 6 На вкладке **Где**, в столбце **Целевое расположение** выберите **Безопасное облачное хранилище**.
Если вы не активировали резервное копирование в облаке, щелкните ссылку **Активировать бесплатно** и следуйте инструкциям.
- 7 На вкладке **Когда** в списке **Расписание** можно выбрать наиболее удобное расписание резервного копирования.
- 8 Выберите **Сохранить параметры**.

Запуск резервного копирования в облаке Norton

Примечание: Norton может отправить запрос на ввод учетных данных для аутентификации при первом выполнении резервного копирования.

- 1 Запустите Norton.
Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.
- 2 В главном окне продукта Norton дважды щелкните **Резервное копирование** и выберите **Выполнить резервное копирование**.
- 3 В окне **Выполнение резервного копирования** следуйте инструкциям, выводимым на экран.
- 4 Нажмите кнопку **Заккрыть**.

Примечание: Если резервное копирование выполнить не удастся, Norton приводит список возможных причин, таких как нехватка места или недостаточная скорость передачи данных. Прежде чем запускать резервное копирование, всегда проверяйте, есть ли соединение с Интернетом и подключены ли устройства хранения.

Добавление и исключение файлов и папок из наборов резервного копирования

Norton позволяет выполнять резервное копирование в наборы файлов различных типов, таких как изображения, музыка, видео и т.д. Можно указать файлы и папки, которые содержат типы файлов, обычно включаемые в наборы, или исключить их из резервного копирования.

Также вы можете добавить или удалить расширения файлов, которые обычно являются частью типов файлов по умолчанию. Дополнительную информацию см. в разделе См. ["Просмотр и изменение типов и расширений файлов по умолчанию, включаемых Norton в резервное копирование"](#) на стр. 79.

Добавление файлов и папок в наборы резервного копирования и их исключение

- 1 Запустите Norton.
Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.
- 2 В главном окне Norton дважды щелкните **Резервное копирование** и выберите **Наборы данных резервного копирования**.

- 3 В окне **Параметры резервного копирования** в раскрывающемся списке **Набор данных резервного копирования** выберите набор данных резервного копирования, который необходимо настроить.
- 4 На вкладке **Что** нажмите кнопку **Добавить или исключить файлы и папки**.
- 5 В появившемся окне выполните следующие действия:
 - Чтобы добавить файл в набор данных резервного копирования, нажмите **Включить файл** и перейдите к файлу, который необходимо добавить.
 - Чтобы добавить папку в набор данных резервного копирования, нажмите **Включить папку** и перейдите к папке, которую необходимо добавить.
 - Чтобы удалить файл из набора данных резервного копирования, нажмите **Исключить файл** и перейдите к файлу, который необходимо удалить.
 - Чтобы удалить папку из набора данных резервного копирования, нажмите **Исключить папку** и перейдите к папке, которую необходимо удалить.
- 6 В окне **Параметры резервного копирования** нажмите **Сохранить параметры**.

Примечание: Вы также можете щелкнуть правой кнопкой мыши файл или папку и выбрать из контекстного меню **Norton Security > Добавить в резервное копирование/Исключить из резервного копирования**.

Пункты **Добавить в резервную копию** и **Исключить из резервного копирования** появляются в контекстном меню, только если настроено резервное копирование и закрыты окна **Параметры резервного копирования** и **Восстановление файлов**.

Просмотр и изменение типов и расширений файлов по умолчанию, включаемых Norton в резервное копирование

По умолчанию перед запуском резервного копирования Norton ищет файлы, имеющие определенный тип — такие как рисунки, музыка или видео. Типы файлов по умолчанию позволяют автоматически сохранять при создании набора резервного копирования и его запуске те файлы, которые большинство пользователей считает важными. Для включения данных в резервные копии и их исключения вы можете изменить типы файлов по умолчанию, включаемых в резервное копирование, а также расширения файлов, относящихся к каждому из типов.

Просмотр и изменение типов и расширений файлов по умолчанию, включаемых в резервное копирование

- 1 Запустите Norton.
Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.
- 2 В главном окне Norton дважды щелкните **Резервное копирование** и выберите **Наборы данных резервного копирования**.
- 3 В окне **Параметры резервного копирования** в раскрывающемся списке **Набор данных резервного копирования** выберите набор данных резервного копирования, который необходимо настроить.
- 4 На вкладке **Что** выберите пункт **Изменить тип файла**, чтобы изменить расширения, включенные в типы файлов для изображений, звуковых и видеофайлов, а также другие типы файлов.
- 5 В поле **Типы файлов** рядом с типом файлов нажмите кнопку **Настроить**.
- 6 В появившемся окне выполните следующие действия и нажмите **Сохранить**.
 - Чтобы удалить расширение файла, выберите в списке расширение файла и нажмите **Удалить**.
 - Нажмите **Добавить новые**, чтобы добавить в список дополнительные расширения.
- 7 В окне **Параметры резервного копирования** нажмите **Сохранить параметры**.

Восстановление изображений, музыки или других важных файлов из наборов данных резервного копирования Norton

Вы можете легко восстановить данные резервного копирования Norton, когда ваш компьютер атакован программой-вымогателем или иной вредоносной программой, или если в аппаратном обеспечении возникает неустранимый сбой. Вы можете выбрать восстановление полных наборов данных резервного копирования или определенных файлов в наборе. Вы также можете указать путь хранения восстановленных файлов.

Примечание: Восстановление происходит в соответствии с настроенным набором данных резервного копирования. При выполнении восстановления на новое устройство не следует ожидать, что Norton восстановит ваши файлы в соответствии с желаемой структурой папок на вашем старом устройстве.

Восстановление файлов резервных копий Norton или полных наборов данных резервного копирования

- 1 Запустите Norton.
Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.
- 2 В главном окне Norton дважды щелкните **Резервное копирование** и выберите **Восстановить файлы**.
- 3 В окне **Восстановить файлы** в разделе **Восстановить из** выберите пункт **Показать все**.
Выберите набор данных резервного копирования и нажмите **ОК**.
- 4 В окне **Восстановить файлы** найдите раздел **Файлы** и нажмите кнопку **Выбор файлов и папок**.
Выберите файлы для восстановления и нажмите кнопку **ОК**.
- 5 В окне **Восстановить файлы** найдите раздел **Восстановить в** и нажмите **Исходное расположение**.
Нажмите **Изменить** и следуйте инструкциям, если не хотите восстанавливать файлы в исходное расположение.
- 6 Нажмите **Восстановить файлы**, а затем **Заккрыть**.

Загрузка файлов из резервного копирования в облаке

- 1 Перейдите на веб-сайт <https://my.Norton.com>.
- 2 Нажмите **Вход**.
- 3 Введите связанный с вашей учетной записью NortonLifeLock адрес эл. почты и пароль, затем нажмите **Войти**.
- 4 На странице **Мой Norton** на плитке **Резервное копирование в облаке** нажмите **Показать наборы данных рез. копир**.
- 5 Выберите набор данных резервного копирования, содержащий файл, который необходимо загрузить.
- 6 Перейдите к нужному файлу.
Если вам известно имя файла, вы можете использовать функцию поиска, чтобы найти конкретный файл.
Используйте параметр **Фильтр**, чтобы отфильтровать изображения и документы.
- 7 Наведите указатель мыши на имя файла и щелкните **Загрузить**.

Удаление набора данных из резервного копирования в облаке

Ненужные наборы данных резервного копирования можно удалить. Единственный набор данных резервного копирования удалить нельзя. Однако перед удалением старого набора данных резервного копирования можно создать новый набор.

Примечание: Иногда из-за сбоя серверной службы или обслуживания сервера у вас могут возникнуть проблемы с удалением данных резервного копирования. В таких случаях попробуйте удалить данные позднее. Чтобы определить наличие сбоев службы, посетите страницу [Состояние службы Norton](#).

При удалении набора данных резервного копирования также изменяются и сведения о файлах, включенных в этот набор. Например, появляется значок, а со страницы свойств файла пропадает вкладка **Резервное копирование**.

Как правило, набор данных резервного копирования удаляется с целью освобождения памяти в безопасном облачном хранилище.

Примечание: Чтобы удалить набор данных резервного копирования из облачного хранилища, необходимо для параметра **Ограничение использован. сети** в окне **Параметры брандмауэра** задать значение **Без ограничений**.

Дополнительную информацию см. в разделе См. "[Ограничение использования Интернета для Norton](#)" на стр. 72.

Удаление набора данных резервного копирования

- 1 Запустите Norton.
Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.
- 2 В главном окне Norton дважды щелкните **Резервное копирование** и выберите **Наборы данных резервного копирования**.
- 3 В окне **Параметры резервного копирования** в раскрывающемся списке **Набор данных резервного копирования** выберите набор данных резервного копирования, который необходимо удалить.
- 4 Нажмите кнопку **Удалить**.
- 5 В окне **Удал. набор данных резер. копир.** выполните одно из следующих действий:
 - Чтобы удалить текущий набор данных резервного копирования, выберите **Удалить набор данных резервного копирования**.

- Чтобы удалить текущий набор данных резервного копирования и удалить уже созданные файлы резервной копии, выберите **Удалить набор данных резервного копирования и файлы**.

6 Нажмите кнопку **Да**.

Удаление набора данных резервного копирования из учетной записи

- 1 Войдите в свою [учетную запись](#).
- 2 На странице **Мой Norton** нажмите **Резервное копирование в облаке**.
Будут показаны используемые наборы резервного копирования.
- 3 Для удаления набора резервного копирования нажмите на значок корзины рядом с набором резервного копирования, который нужно удалить.
- 4 В окне подтверждения **Удалить набор данных резервного копирования** нажмите **Удалить**.
Нажмите **Отмена**, чтобы вернуться на предыдущую страницу без удаления набора данных.

Настройка параметров продукта Norton

В окне **Параметры** можно включить или выключить следующие **службы быстрого управления** :

- **Режим без вывода сообщений**
- **Резервное копирование**
- **Отобр. состояния рез. копирования**
- **Автоматический запуск LiveUpdate**
- **Интеллектуальный брандмауэр**
- **Защита от изменений Norton**

Рекомендуется не выключать никакие службы за исключением режима без вывода сообщений.

Включение и выключение служб быстрого управления Norton

- 1 Запустите Norton.
Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.
- 2 В главном окне Norton щелкните **Параметры**.
- 3 В окне **Параметры** в разделе **Быстрое управление** выполните одно из следующих действий:

- Для включения службы отметьте переключатель.
- Для выключения службы отмените выбор переключателя.
Если появляется предупреждение или сообщение, выберите продолжительность в раскрывающемся меню и нажмите кнопку **ОК**.

Настройка параметров защиты в реальном времени

Защита в реальном времени обнаруживает неизвестные угрозы безопасности на вашем компьютере и позволяет выбрать, какие действия предпринять в случае обнаружения.

Примечание: Для большинства пользователей подходят значения по умолчанию. Если требуется временно выключить компонент, как можно быстрее включите его обратно. Для автоматического удаления элементов с низкой степенью риска настройте расширенный режим SONAR. Функция автоматической защиты проверяет программы на наличие вирусов и угроз безопасности при их запуске. Выключать автоматическую защиту не рекомендуется.

Настройка автоматической защиты для сканирования съемных носителей

Проверять на наличие загрузочных вирусов при обращении к съемному носителю. Повторное сканирование носителя, проверенного на предмет загрузочного вируса, выполняется только после его форматирования или повторной установки в устройство. Если вы подозреваете, что съемный носитель заражен загрузочным вирусом, включите автоматическую защиту, чтобы выполнить сканирование носителя повторно. Вставьте носитель в устройство и откройте его с помощью окна "Мой компьютер", чтобы функция автоматической защиты выполнила его сканирование. Кроме того, сканирование носителя можно запустить вручную, чтобы убедиться, что съемный носитель не заражен.

Настройка параметров автоматической защиты

- 1 Запустите Norton.
Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.
- 2 В главном окне Norton щелкните **Параметры**.
- 3 В окне **Параметры** выберите **Защита от вирусов**.
- 4 В разделе **Сканирование съемных носителей**, установите ползунок на значение **Вкл**.

Настройка SONAR для автоматического удаления угроз

SONAR обеспечивает защиту в реальном времени от угроз, выполняя превентивный поиск неизвестных угроз на компьютере. SONAR распознает новые угрозы, исходя из

поведения приложений. В параметрах расширенного режима SONAR можно настроить, каким образом SONAR удаляет угрозы.

Настройка SONAR для автоматического удаления угроз

- 1 Запустите Norton.
 Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.
- 2 В главном окне Norton щелкните **Параметры**.
- 3 В окне **Параметры** выберите **Защита от вирусов**.
- 4 В разделе **Автоматически удалять угрозы** переместите ползунок в положение **Всегда**.
- 5 В разделе **Удалять угрозы, если меня нет на месте** переместите ползунок в положение **Всегда**.
- 6 Нажмите кнопку **Применить**.

Настройка автоматической защиты для исключения известных безопасных файлов из сканирования Norton

Если есть основания полагать, что Norton распознает разрешенное приложение как угрозу безопасности, то соответствующий файл можно исключить из сканирования Norton.

Исключение файлов из сканирований Norton

- 1 Запустите Norton.
 Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.
- 2 В главном окне Norton щелкните **Параметры**.
- 3 В окне **Параметры** выберите **Защита от вирусов**.
- 4 В окне параметров Антивирусная программа откройте вкладку **Сканирования и угрозы**.
- 5 В разделе **Исключения / Угрозы с низкой степенью риска** выполните одно из следующих действий:
 - В строке **Элементы, исключаемые из сканирования** нажмите кнопку **Настроить**.
 - В строке **Элементы для исключения из сканирований автоматической защиты, SONAR и контроля загрузок** нажмите кнопку **Настроить**.
- 6 В открывшемся окне выберите **Добавить папки** или **Добавить файлы**.

- 7 В окне **Добавить элемент** щелкните по значку обзора. В открывшемся диалоговом окне выберите элемент, который требуется исключить из сканирований.
- 8 Нажмите кнопку **ОК**.

Подробнее о параметрах Сканирования и угрозы

С помощью параметров **Сканирования и угрозы** можно настроить операции сканирования, выполняемые продуктом Norton на компьютере. Можно настроить сканирования на основании цифровой подписи и уровня надежности файлов, имеющихся в вашем компьютере. Можно задать параметры сканирования почтовых сообщений продуктом Norton.

Доступны следующие параметры **Сканирования и угрозы**.

Сканирование компьютера

Продукт позволяет выполнять различные типы операций сканирования для выявления и устранения заражений компьютера. Можно использовать следующие виды сканирования: быстрое сканирование, полное сканирование системы и выборочное сканирование. Для настройки **операций сканирования**, выполняемых продуктом Norton на компьютере, предусмотрен широкий набор параметров. Также можно задать сканирование сжатых файлов.

С помощью параметров **Сканирования компьютера** можно настроить сканирование для поиска руткитов, других скрытых объектов, следящих cookie и неизвестных угроз безопасности. Предусмотрены следующие параметры.

- **Сканирование сжатых файлов**

Сканирует и исправляет содержимое сжатых файлов.

Когда эта функция включена, Norton сканирует файлы, расположенные внутри сжатых файлов, проверяет их на наличие вирусов и других угроз безопасности и удаляет сжатые файлы.

- **Сканирование на наличие руткитов и скрытых объектов**

Сканирует компьютер на наличие руткитов и других скрытых угроз безопасности

- **Сканирование сетевых дисков**

Позволяет выполнить сканирование сетевых дисков, подключенных к компьютеру.

Norton выполняет **сканирование сетевых дисков** в ходе **полного сканирования** и **выборочного сканирования**. По умолчанию параметр **Сканирование сетевых дисков** включен. Если выключить его, то Norton не будет выполнять сканирование сетевых дисков.

- **Эвристическая защита**

Сканирует компьютер для его защиты от неизвестных угроз безопасности.

Norton использует эвристическую технологию для проверки подозрительных характеристик файлов, классифицированных как зараженные. Эта технология сравнивает характеристики файла с характеристиками известного зараженного файла. Если многие характеристики файлов совпадают, то Norton классифицирует файл как зараженный угрозой.

- **Сканирование на наличие следящих Cookie**
Сканирует компьютер на наличие небольших файлов, добавляемых программами для отслеживания операций пользователя.
- **Полное сканирование системы**
При полном сканировании системы выполняется тщательная проверка всего компьютера на наличие вирусов, программ-шпионов и различных уязвимостей. С помощью параметра **Настроить** можно запланировать полное сканирование системы.

Защищенные порты

Параметры защищенных портов позволяют защитить порты POP3 и SMTP, используемые почтовой программой.

Этот параметр можно использовать, чтобы вручную настроить порты электронной почты POP3 и SMTP для защиты электронной почты. Если номера портов SMTP и POP3, предоставленные поставщиком услуг Интернета (ISP), отличаются от стандартных номеров портов SMTP и POP3, необходимо настроить Norton для защиты соответствующих портов.

Сканирование электронной почты на наличие вирусов

Функция сканирования электронной почты на наличие вирусов защищает от угроз, пересылаемых во вложениях электронной почты.

С помощью параметров сканирования электронной почты с помощью антивирусной программы можно настроить сканирование почтовых сообщений в продукте Norton. Norton автоматически сканирует отправляемые и принимаемые почтовые сообщения с учетом этих параметров.

Исключения / Угрозы с низкой степенью риска

В параметрах исключений указываются такие объекты, как папки, файлы или диски, которые необходимо исключить из сканирований, выполняемых Norton. К таким объектам относятся сигнатуры сканирования и угрозы с низкой степенью риска.

В параметрах исключений можно выбрать категории угроз, которые должны выявляться продуктом Norton. Предусмотрены следующие параметры.

- **Угрозы с низкой степенью риска**
Позволяет управлять элементами с низкой степенью угроз, которые найдены на компьютере.

Можно указать, каким образом продукт Norton должен реагировать на несущественные угрозы.

- **Элементы для исключения из сканирования**

Позволяет указать диски, папки и файлы, которые не нужно сканировать на наличие угроз.

Можно как добавить новые исключения, так и изменить ранее исключенные объекты. При необходимости можно удалить объект из списка исключений.

- **Элементы для исключения из сканирований автоматической защиты, SONAR и контроля загрузок**

Позволяет указать диски, папки и файлы, которые требуется исключить из сканирований функций автоматической защиты и SONAR.

Можно добавить новые объекты для исключения и изменить объекты, добавленные ранее. При необходимости можно удалить объект из списка исключений.

- **Сигнатуры для исключения из сканирования**

Позволяет выбрать известную угрозу по имени или удалить имя угрозы из списка исключенных элементов.

При необходимости можно просмотреть степень влияния угрозы с точки зрения быстрого действия, конфиденциальности, простоты удаления и скрытности.

- **Очистить ИД файлов, исключаемых во время сканирования**

Позволяет удалить информацию о репутации файлов, которые исключены из сканирования.

С помощью опции **Очистить все** можно очистить информацию о репутации файлов, которые исключены из сканирования.

Примечание: Исключения ослабляют защиту, поэтому их следует использовать только в случае крайней необходимости.

Подробнее о параметрах предотвращения вторжений и защиты браузера

Система предотвращения вторжений сканирует получаемые и отправляемые пакеты и сравнивает их с набором сигнатур атак. Сигнатуры атаки содержат наборы данных, сигнализирующие о намерении злоумышленника использовать слабое место в защите операционной системы или программы. Система предотвращения вторжений защищает компьютер от наиболее распространенных атак из Интернета.

Если информация соответствует известной сигнатуре атаки, то система предотвращения вторжений автоматически уничтожает пакет и прерывает соединение с компьютером, отправившем данные. Таким образом обеспечивается надежная защита компьютера.

Для обнаружения и блокировки подозрительных сетевых операций система предотвращения вторжений применяет заранее составленный список сигнатур атак. Продукт Norton регулярно обновляет список сигнатур атак с помощью функции LiveUpdate. Если функция автоматического запуска LiveUpdate не используется, то рекомендуется запускать LiveUpdate раз в неделю.

Кроме того, продукт Norton обеспечивает защиту веб-браузера от вредоносных программ.

Примечание: Компонент защиты веб-браузера доступен для браузеров Google Chrome, Microsoft Internet Explorer, Mozilla Firefox и Microsoft Edge.

Растущая популярность Интернета делает веб-браузер привлекательной мишенью для атак с вредоносных веб-сайтов. Такие веб-сайты находят и используют уязвимые места веб-браузера для загрузки вредоносных программ в систему без ведома пользователя. Такие вредоносные программы иначе называют скрытными загрузками. Продукт Norton защищает браузер от загрузок без ведома пользователя с вредоносных веб-сайтов.

Параметры **Вторжения и защита браузера** также включают функцию **Контроль загрузок** для защиты компьютера от загрузки небезопасных файлов. Функция контроля загрузок предоставляет информацию об уровне репутации всех исполняемых файлов, загружаемых браузером. Функция "Контроль загрузок" поддерживает загрузку только по протоколу HTTPS с использованием браузеров Internet Explorer 6.0, Edge 40.15063, Chrome 10.0, Firefox 3.6 или их более поздних версий. Сведения о репутации, предоставляемые функцией контроля загрузок, служат индикатором того, насколько безопасно устанавливать загруженный файл. Эти сведения позволяют вам решить, устанавливать ли исполняемый файл.

Установите параметры Norton таким образом, чтобы вы могли удаленно управлять защищаемыми устройствами

Функция **удаленного управления** Norton отправляет информацию о состоянии вашего устройства и другие данные в приложение Norton Studio для Windows. Это приложение можно использовать для просмотра, управления и изучения продуктов Norton, а также для удаленного решения определенных проблем с защитой устройства. По умолчанию функция удаленного управления выключена.

Включение удаленного управления

- 1 Запустите Norton.

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

- 2 В главном окне продукта Norton щелкните **Параметры**.
- 3 В окне **Параметры** нажмите **Параметры администрирования**.

- 4 В строке **Удаленное управление** переместите переключатель в положение **Вкл.**
- 5 Нажмите кнопку **Применить**, а затем — кнопку **Заккрыть**.

Защита параметров безопасности устройства Norton от несанкционированного доступа

Для предотвращения несанкционированного изменения параметров безопасности на устройстве Norton включите **Защиту параметров паролем** и **Защиту от изменений продукта Norton**.

- **Защита параметров паролем** позволяет установить пароль, который будет запрашиваться при просмотре или изменении параметров безопасности устройства.
- **Защита от изменений продукта Norton** отслеживает внесение изменений в параметры неизвестными или подозрительными приложениями.

Включение и выключение функций защиты параметров паролем и защиты от изменений продукта Norton

- 1 Запустите Norton.
Если отображается окно **Мой Norton** рядом с разделом **Безопасность устройства**, нажмите **Открыть**.
- 2 В главном окне продукта Norton щелкните **Параметры**.
- 3 В окне **Параметры** нажмите **Параметры администрирования**.
- 4 В разделе **Безопасность продукта** :
 - В строке **Защита параметров паролем** переместите переключатель в положение **Вкл.** или **Выкл.**
 - В строке **Защита от изменений продукта Norton** переместите переключатель в положение **Вкл.** или **Выкл.**
Если появится соответствующий запрос, введите продолжительность периода, в течение которого этот компонент должен быть выключен, а затем нажмите кнопку **ОК**.
- 5 Нажмите кнопку **Применить**.
- 6 Будет открыто окно **Задать пароль**, в котором необходимо ввести и подтвердить пароль. Вам нужно устанавливать пароль каждый раз при включении и отключении функции.
- 7 Нажмите кнопку **ОК**.
- 8 В окне **Параметры** нажмите кнопку **Заккрыть**.

Сброс утерянного или забытого пароля функции защиты параметров паролем

Чтобы получить доступ к параметрам и установить новый пароль, необходимо переустановить Norton.

Установка сочетания клавиш для поиска информации в компоненте «Безопасность устройства Norton»

При выполнении поиска с помощью значка поиска в приложении Norton Защита устройства можно найти полезную информацию как об отдельных компонентах, так и на общие темы. Для быстрого поиска можно использовать **Ctrl + F** или настроить собственное сочетание.

Настройка сочетания клавиш для функции поиска

1 Запустите Norton.

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

2 В главном окне продукта Norton щелкните **Параметры**.

3 В окне **Параметры** нажмите **Параметры администрирования**.

4 В строке **Сочетание клавиш для функции поиска** переместите переключатель в положение **Вкл**.

5 Нажмите стрелку и выберите клавишу, которую вы хотите назначить для поиска средствами продукта.

6 Выполните одно из следующих действий:

- Для того, чтобы сочетание клавиш работало только тогда, когда окно продукта Norton активно, **снимите флажок** у параметра **Везде**.
- Для того, чтобы сочетание клавиш работало даже тогда, когда окно продукта Norton **неактивно**, **установите флажок** у параметра **Везде**.

7 Нажмите кнопку **Применить**, а затем — кнопку **Заккрыть**.

Оптимизация компьютера для игр при помощи Game Optimizer

Game Optimizer¹ — запатентованная технология для ПК с многоядерными процессорами. Она обеспечивает захватывающий игровой процесс благодаря сокращению скачков быстродействия и поддерживает безопасность вашего компьютера. Ограничивая менее

важные приложения одним ядром процессора, эта технология позволяет предоставить остальные ресурсы ЦП игре.

Примечание: Для использования Game Optimizer процессор вашего компьютера должен иметь как минимум четыре ядра.

Game Optimizer помогает улучшить игровой процесс следующим образом:

- Оптимизирует быстродействие процессора для более комфортной игры.
- Ограничивает менее важные приложения одним ядром процессора, чтобы выделить остальные ресурсы ЦП игре для повышения быстродействия.
- Автоматически обнаруживает игры.²
- Позволяет добавлять игры или выбирать игры, которые не нужно оптимизировать.
- Увеличивает частоту кадров в секунду и снижает задержки.
- Устраняет необходимость отключать антивирусную защиту, распределяя ресурсы процессора для оптимальной игровой производительности.
- Выделяя ядра процессора игре, сокращает внезапные пиковые нагрузки процессора, которые могут замедлить игру.

Дополнительную информацию см. в статье См. ["Подробнее о Game Optimizer"](#) на стр. 93..

Примечание: Все важные компоненты "Защиты Norton", которые ограждают ваш компьютер от вирусов и угроз безопасности, работают в фоновом режиме, не отвлекая вас от игры.

Настройка Norton для оптимального процесса игры

- 1 Запустите Norton.
- 2 В окне **Мой Norton** на центральной панели нажмите значок молнии.
- 3 На **Панели игр** нажмите **Управление оптимизацией**.
- 4 В окне **Game Optimizer** настройте следующие параметры:
 - **Ограничить использование ресурсов для процессов пользователя** : включите этот параметр, чтобы ограничить использование ЦП для всех процессов, инициируемых пользователем.
 - **Ограничить использование ресурсов для системных процессов** : включите этот параметр, чтобы ограничить использование ЦП для всех процессов, инициируемых операционной системой.

- **Автоматически установить схему управления питанием на максимальную производительность** : включите этот параметр, чтобы переключиться на высокопроизводительную схему управления питанием в Windows. Game Optimizer создает настраиваемые параметры схемы управления питанием Windows, чтобы максимизировать быстродействие в играх. Эта схема управления питанием доступна только во время игрового сеанса. После завершения игрового сеанса для схемы электропитания по умолчанию используется исходная настройка. Norton рекомендует оставить этот параметр включенным для оптимизации процесса игры.
- **Оптимизированные игры** : список игр, оптимизированных Game Optimizer.

Выключение Game Optimizer

По умолчанию компонент Game Optimizer включен. Вы можете отключить Game Optimizer, если не хотите, чтобы он улучшал игровой процесс. Norton рекомендует оставить этот компонент включенным для оптимизации процесса игры.

Включение и выключение Game Optimizer

- 1 Запустите Norton.
- 2 В окне **Мой Norton** на левой панели переместите переключатель **Game Optimizer**, чтобы включить или выключить компонент.

Включение или выключение Game Optimizer в области уведомлений

- ◆ В области уведомлений на панели задач Windows щелкните правой кнопкой значок Norton и выполните одно из следующих действий:
 - Чтобы отключить Game Optimizer, нажмите **Отключить Game Optimizer**.
 - Чтобы включить Game Optimizer, нажмите **Включить Game Optimizer**.

¹Компонент Game Optimizer доступен только в Windows (за исключением Windows 10 в S-режиме и Windows с процессором ARM) с как минимум четырехъядерными процессорами.

²Автоматически обнаруживает игры с помощью режима полноэкранный обнаружения с высокой загрузкой ЦП, а также программ запуска игр³, если пользователь добавляет игру вручную или она была обнаружена ранее.

³По состоянию на апрель 2021 года поддерживаются следующие программы запуска игр: Bethesda, Blizzard, Epic, ID, Origin, Rockstar, Steam, Uplay.

Подробнее о Game Optimizer

Game Optimizer¹ — запатентованная технология для ПК с многоядерными процессорами. Она обеспечивает захватывающий игровой процесс благодаря сокращению скачков

быстродействия и поддерживает безопасность вашего компьютера. Ограничивая менее важные приложения одним ядром процессора, она позволяет предоставить остальные ресурсы ЦП игре.

Game Optimizer помогает улучшить игровой процесс следующим образом:

- Оптимизирует быстродействие процессора для более комфортной игры.
- Ограничивает менее важные приложения одним ядром процессора, чтобы выделить остальные ресурсы ЦП игре для повышения быстродействия.
- Автоматически обнаруживает игры.²
- Позволяет добавлять игры или выбирать игры, которые не нужно оптимизировать.
- Увеличивает частоту кадров в секунду и снижает задержки.
- Устраняет необходимость отключать антивирусную защиту, распределяя ресурсы процессора для оптимальной игровой производительности.
- Выделяя ядра процессора игре, сокращает внезапные пиковые нагрузки процессора, которые могут замедлить игру.

Минимизация фоновых операций позволяет повысить быстродействие компьютера, что создает идеальные условия для игры. После завершения игрового сеанса Norton 360 for Gamers возобновляет все приостановленные действия в фоновом режиме.

Примечание: Для использования Game Optimizer процессор вашего компьютера должен иметь как минимум четыре ядра.

Game Optimizer начинает оптимизацию при запуске игрового приложения, выполняя ее до выхода из игры. Оптимизация приостанавливается, если вы выходите из полноэкранного режима во время активного игрового сеанса. Например, если вы нажмете **Alt + Tab** для доступа к любой другой запущенной программе, Norton остановит оптимизацию игры и отменит ограничения. Но когда вы вернетесь к игре, оптимизация возобновится, и ограниченные программы лишатся возможности использования ЦП.

Примечание: Все важные компоненты "Защиты Norton", которые ограждают ваш компьютер от вирусов и угроз безопасности, работают в фоновом режиме, не отвлекая вас от игры.

Вы можете увидеть статус Game Optimizer в области уведомлений на панели задач. На значке продукта Norton в области уведомлений отображается зеленая молния, когда Game Optimizer работает. При выключении Game Optimizer цвет меняется на серый.

На панели Gamer Dashboard отображается состояние Game Optimizer, статус оптимизации недавних игр и доступ к параметрам Game Optimizer. Вы можете использовать переключатель, чтобы включить или отключить оптимизацию для недавних игр.

Примечание: Компонент Game Optimizer доступен только в Norton 360 for Gamers.

¹Компонент Game Optimizer доступен только в Windows (за исключением Windows 10 в S-режиме и Windows с процессором ARM) с как минимум четырехъядерными процессорами.

²Автоматически обнаруживает игры с помощью режима полноэкранный обнаружения с высокой загрузкой ЦП, а также программ запуска игр³, если пользователь добавляет игру вручную или она была обнаружена ранее.

³По состоянию на апрель 2021 года поддерживаются следующие программы запуска игр: Bethesda, Blizzard, Epic, ID, Origin, Rockstar, Steam, Uplay.

Как вручную добавить игры в список оптимизированных игр

Game Optimizer¹ — запатентованная технология для ПК с многоядерными процессорами. Она обеспечивает захватывающий игровой процесс благодаря сокращению скачков быстродействия и поддерживает безопасность вашего компьютера. Ограничивая менее важные приложения одним ядром процессора, эта технология позволяет предоставить остальные ресурсы ЦП игре. Game Optimizer автоматически сверяется с внутренним списком известных игр для обнаружения игровых приложений.^{1,2} Если не удастся обнаружить какую-либо игру автоматически, вы можете вручную добавить ее в список **Оптимизированных игр**.

Кроме того, вы можете удалить игры из списка **Оптимизированных игр**, если не хотите, чтобы приложение Norton 360 for Gamers улучшало их быстродействие.

Примечание: Когда вы удаляете определенную игру из списка **Оптимизированных игр**, она перестает быть оптимизированной, что может повлиять на ее работу.

Добавление игры в список оптимизированных игр

- 1 Запустите Norton.
- 2 В окне **Мой Norton** на центральной панели нажмите значок молнии.
- 3 На **Панели игр** нажмите **Управление оптимизацией**.
- 4 В окне **Game Optimizer** рядом с разделом **Оптимизированные игры** нажмите **Добавить**.
- 5 Найдите и выберите игру, которая нуждается в оптимизации Norton.

Удаление игры из списка оптимизированных игр

- 1 Запустите Norton.
- 2 В окне **Мой Norton** на центральной панели нажмите значок молнии.
- 3 На **Панели игр** нажмите **Управление оптимизацией**.
- 4 В окне **Game Optimizer** в разделе **Оптимизированные игры** отключите переключатель рядом с игрой, которую нужно удалить.

¹Компонент Game Optimizer доступен только в Windows (за исключением Windows 10 в S-режиме и Windows с процессором ARM) с как минимум четырехъядерными процессорами.

²Автоматически обнаруживает игры с помощью режима полноэкранного обнаружения с высокой загрузкой ЦП, а также программ запуска игр³, если пользователь добавляет игру вручную или она была обнаружена ранее.

³По состоянию на апрель 2021 года поддерживаются следующие программы запуска игр: Bethesda, Blizzard, Epic, ID, Origin, Rockstar, Steam, Uplay.

Поиск дополнительных решений

В этой главе рассмотрены следующие вопросы:

- [Удаление приложения Защита устройства в Windows](#)
- [Заявления об отказе от ответственности](#)

Удаление приложения Защита устройства в Windows

Следуйте приведенным ниже инструкциям, чтобы удалить приложение Защита устройства с вашего компьютера.

Удаление приложения Защита устройства из Windows

- 1 Используйте сочетание клавиш **Windows + R**, чтобы открыть диалоговое окно **Выполнить**.
- 2 Введите `appwiz.cpl` и нажмите **Enter**.
- 3 В списке установленных программ выберите продукт Norton, а затем щелкните **Удалить/изменить**.
- 4 Следуйте инструкциям, выводимым на экран.

Чтобы полностью удалить Безопасность устройства, необходимо перезапустить компьютер.

Заявления об отказе от ответственности

© NortonLifeLock Inc., 2021 г. Все права защищены. NortonLifeLock, логотип NortonLifeLock, логотип с галочкой, Norton, LifeLock и логотип LockMap являются товарными знаками или зарегистрированными товарными знаками NortonLifeLock Inc. или аффилированных компаний в Соединенных Штатах Америки и других странах. Firefox является товарным знаком Mozilla Foundation. Google Chrome и Android являются товарными знаками Google, LLC. Mac, iPhone и iPad являются товарными знаками Apple Inc. Microsoft и логотип Windows являются товарными знаками Microsoft Corporation в США и (или) других странах. Представление Android Robot заимствовано или модифицировано из общедоступных материалов, созданных в Google, и используется согласно условиям лицензии Creative Commons 3.0 Attribution License. Другие наименования являются товарными знаками соответствующих владельцев.