

## Уведомление о политике конфиденциальности в отношении Продуктов и Сервисов Norton *(в редакции от 7 ноября 2018 г.)*

Настоящее Уведомление следует толковать и применять во взаимосвязи и в дополнение к Глобальному заявлению Symantec-Norton о конфиденциальности. В нем описываются категории данных, собираемых Продуктами и Сервисами Norton, а также цели, в которых обрабатываются эти категории данных. Уведомление предназначено для предоставления обязательной информации о прозрачности как для отдельных пользователей Norton в качестве субъектов данных, так и для корпоративных пользователей Norton — предприятий малого и среднего бизнеса — в качестве контролеров данных. Обратите внимание, что категории данных, отмеченные звездочкой (\*), являются персональными данными, передаваемыми Symantec с целью предоставления соответствующих функций продукта Norton и функциональных возможностей сервиса. Все прочие категории данных собираются программным обеспечением Norton для обработки в неидентифицируемой форме.

Все Продукты и Сервисы Norton соответствуют самым высоким стандартам, предусмотренным [Глобальным заявлением Symantec-Norton о конфиденциальности](#). Кроме того, в целях всестороннего информирования об уникальных характеристиках и предназначении каждого из продуктов и сервисов Norton в дополнение к описанию таких продуктов и сервисов в Уведомлении описан порядок сбора и перечислены цели использования Персональных данных.

В случае если вы не согласны с теми или иными положениями настоящего Уведомления, просим не загружать, не устанавливать и не использовать соответствующие Продукты и Сервисы или их функции и (или) незамедлительно удалить или прекратить использование таких Продуктов и Сервисов или их функций. Применительно к Продуктам и Сервисам, которые требуют предоставления дополнительных Персональных данных или согласия на их обработку в целях использования тех или иных дополнительных функций таких Продуктов и Сервисов, в момент загрузки, установки, активации или использования вышеуказанных функций вам будет предложено ознакомиться с настоящим Уведомлением, с тем чтобы принять взвешенное решение об использовании соответствующих функций.

### Содержание

Norton App Lock .....	2
Norton Clean.....	2
Norton Error Management .....	2
Norton Community Watch.....	4
Norton Core .....	5
Norton Mobile Security.....	6
Norton Security Scan.....	8
Norton Secure Login .....	9
Norton Ultimate Help-Desk и Norton Computer Tune-Up .....	10
Norton Secure VPN (раньше Norton WiFi Privacy) .....	11
Средства обеспечения безопасности Norton (Security, Internet Security, One, Antivirus и 360) .....	12
Norton Safe Search, Norton Home Page, Norton Safe Web .....	13
Norton Security Toolbar.....	15
Norton Identity Safe.....	16
Norton Family Premier.....	17

## Norton App Lock

Описание Продукта или Сервиса	Условия доступа и сбора данных	Обработка информации
<p>Norton App Lock позволяет пользователю ограничивать доступ и защищать мобильные приложения от несанкционированного использования посредством задания специального кода, пароля или схемы доступа. App Lock можно настроить таким образом, чтобы в случае кражи или утери мобильного устройства (при наличии такой возможности) фронтальная камера устройства делала снимок пользователя после трех неудачных попыток разблокировки.</p>	<p>*1. Адрес электронной почты пользователя</p> <p>2. Установленные пользователем PIN-коды, пароли для мобильных приложений</p> <p>3. По выбору пользователя — изображения на основе настроек</p>	<p>1. Адрес электронной почты пользователя необходим Symantec для восстановления и сброса пароля доступа к Norton App Lock.</p> <p>2. 3. Любые другие данные, вводимые пользователем при использовании продукта, хранятся на пользовательском устройстве.</p>

## Norton Clean

Описание Продукта или Сервиса	Условия доступа и сбора данных	Обработка информации
<p>Norton Clean — приложение, обеспечивающее наличие достаточного свободного пространства в кэш-памяти мобильного устройства пользователя за счет удаления рекламы и других нежелательных данных и освобождения дополнительного объема памяти.</p>	<p>Международный идентификационный номер мобильного устройства (IMEI)</p>	<p>Symantec получает IMEI от устройства. Хеширование IMEI выполняется сразу же после передачи и перед дальнейшей обработкой. При обработке хеша обеспечивается контроль уникального использования продукта. Таким образом, установить пользователя или устройство, с которого были получены исходные данные, невозможно.</p>

## Norton Error Management

Описание Продукта или Сервиса	Условия доступа и сбора данных	Обработка информации
<p>Norton Error Management регистрирует ошибки в работе Продуктов Norton. В этом случае пользователь имеет возможность сообщить об ошибке Symantec.</p>	<p>1. Информация о состоянии ПК (язык системы, страна местонахождения и версия операционной системы)</p> <p>2. Выполняемые процессы, их статус и параметры работы</p> <p>3. Данные из файлов и папок, которые были открыты на момент обнаружения сбоев в работе продуктов Norton</p>	<p>1.-2.-3. Системные данные обрабатываются Symantec для исправления обнаруженных ошибок и усовершенствования параметров работы Продуктов Norton.</p> <p>В определенных случаях, если выявленные ошибки связаны с угрозами системе безопасности или уязвимостью системы, Symantec может получать и обмениваться со своими партнерами, занимающимися вопросами безопасности в киберпространстве (включая научно-исследовательские организации и поставщиков ПО, призванного обеспечивать безопасность), определенной информацией, которая не позволяет установить или идентифицировать конкретного пользователя. Цель такого обмена заключается в повышении степени информированности, обнаружении и предотвращении возникновения подобных рисков в будущем. Symantec также может использовать статистические данные, полученные в результате обработки вышеупомянутой информации, для отслеживания и публикации отчетов о тенденциях в сфере рисков, связанных с нарушением безопасности.</p>



## Norton Community Watch

Описание Продукта или Сервиса	Условия доступа и сбора данных	Обработка информации
<p>Norton Community Watch позволяет пользователям средств обеспечения безопасности Norton более эффективно идентифицировать новые угрозы безопасности и сводить к минимуму время, затрачиваемое на принятие ответных мер. Программа выборочно собирает данные безопасности и информацию о работе приложений и передает эти сведения Symantec для обработки и выявления новых угроз и их источников. Данное программное обеспечение позволяет создавать более надежные и качественные средства обеспечения безопасности за счет анализа отправляемых пользователями данных.</p> <p>Участвуя в программе Norton Community Watch:</p> <ol style="list-style-type: none"> <li>1. вы помогаете накапливать необходимые данные и разрабатывать более качественные средства защиты против киберугроз, предоставляя всю необходимую информацию наряду с другими участниками программы. Для оценки безопасности каждого загружаемого, сохраняемого или открываемого вами файла наши серверы используют сложные алгоритмы; при этом предлагаемые решения не касаются вас или каких-либо других пользователей лично. Пользователи средств обеспечения безопасности Norton пользуются всеми преимуществами этой новой инновационной технологии, когда продукты Norton:             <ul style="list-style-type: none"> <li>*а. благодаря Download Insight блокируют загружаемые файлы, содержащие вредоносное ПО. Norton сообщает о том, считаются загружаемые файлы безопасными или нет, или об обнаружении неизвестного профиля безопасности. Если загружаемый файл безопасным не является, продукты Norton незамедлительно принимают меры для вашей защиты;</li> <li>b. обеспечивают повышенную скорость обнаружения и сводят к минимуму ложные результаты;</li> <li>*с. благодаря Norton Insight быстрее сканируют и определяют заведомо безопасные файлы, которые уже были переданы, обработаны и разрешены к использованию через Norton Community Watch.</li> </ul> </li> <li>2. предоставляя важные сведения о работе приложений и безопасности, вы участвуете в создании базы данных, необходимой для выявления и нейтрализации новых угроз до того, как они получат широкое распространение.</li> </ol> <p>* Norton Insight доступен только в ОС Windows.</p>	<ol style="list-style-type: none"> <li>1. Идентификатор машины (данные, генерируемые Symantec)</li> <li>2. Серийный номер продукта (присваивается вашему продукту Symantec)</li> <li>3. Номер учетной записи Norton (данные, генерируемые Symantec)</li> <li>*4. Пути к файлам</li> <li>*5. Неисполняемые и переносимые исполняемые файлы, отнесенные к категории вредоносного ПО</li> <li>6. Адреса веб-сайтов, которые открывал пользователь и которые отнесены продуктом Norton к потенциально мошенническим страницам</li> <li>7. Адрес последнего открытого пользователем веб-сайта до установки на ПК загруженного файла с вредоносным ПО</li> <li>8. Сведения о выполняемых процессах и открываемых на устройстве пользователя приложениях, в том числе в момент обнаружения предположительно вредоносного ПО</li> <li>9. Выборка данных, отправленных устройством пользователя в ответ на обнаружение предположительно вредоносного ПО</li> </ol>	<p>Norton Community Watch — сервис, который со стороны сервера размещен и управляется Symantec. Таким образом, все собираемые данные передаются Symantec в следующих целях:</p> <ol style="list-style-type: none"> <li>1. Идентификатор машины необходим для отслеживания количества уникальных устройств, которые используют продукт на основании отдельного взятого соглашения о подписке. Это позволяет контролировать и обеспечивать надлежащее осуществление лицензионных прав.</li> <li>2. Серийный номер продукта присваивается каждому пользователю и предназначен для контроля использования каждого из продуктов исключительно на основании лицензии Symantec.</li> <li>3. Номер учетной записи Norton необходим для отслеживания числа пользователей, подписавшихся на тот или иной продукт Norton.</li> <li>4.-5. Пути к файлам, неисполняемые и переносимые исполняемые файлы призваны обеспечить идентификацию источника и логического места нахождения киберугроз, целью или источником которых является устройство пользователя.</li> <li>6.-7. Адреса веб-сайтов позволяют установить источники потенциальных угроз для системы безопасности в сети Интернет и гарантировать способность Продуктов и Сервисов Symantec обнаруживать вредоносные действия и события, мошеннические веб-сайты, используемое в целях совершения преступлений ПО и другие виды угроз для системы безопасности при работе в сети Интернет.</li> <li>8.-9. Сведения об устройстве необходимы для того, чтобы расширить используемую Symantec базу данных об угрозах. Кроме того, обработка такой информации позволяет повысить степень защиты пользователей Продуктов и Сервисов Symantec в будущем и проводить статистический анализ, изучая имеющиеся тенденции в области кибербезопасности.</li> </ol>

## Norton Core

Описание Продукта или Сервиса	Условия доступа и сбора данных	Обработка информации
<p>Norton Core — беспроводной маршрутизатор, защищающий подключенные к маршрутизатору устройства от вредоносного ПО, вирусов, хакерских атак и других киберугроз.</p>	<p>*1. Идентификатор набора служб (SSID)/пароль (зашифрованный)</p> <p>2. Информация об устройстве, включая Персональные данные, указанные пользователем при задании имени устройства; ФИО или имя-псевдоним лица, которому передано устройство (при условии, что эти сведения указаны пользователем); сведения о пользовательском посреднике устройства (приложения), включая тип, производителя и модель устройства, операционную систему и IP-адрес</p> <p>3. Сведения об использовании устройства, включая время последнего использования, время в сети Интернет по каждому подключенному устройству и протоколы шлюзов с указанием подключений к сети</p> <p>4. Данные и настройки родительского контроля, заданные пользователем, включая заблокированные веб-сайты, посещенные веб-сайты, сведения о фильтрации по времени и содержанию и адреса веб-сайтов, которые представляют или могут представлять опасность</p> <p>*5. Персональные данные, предоставляемые пользователем при создании учетной записи Norton, включая имя и графическое представление пользователя (по желанию)</p> <p>*6. Персональные данные, предоставляемые пользователем в целях оказания услуг поддержки и содействия при подключении, например идентификационный номер, ФИО, тип учетной записи, выбранные пользователем правила и данные об устройстве</p>	<p>1. Данные о параметрах беспроводной сети обрабатываются применительно к заданным пользователем параметрам конфигурации сети WiFi.</p> <p>2. Информация об устройстве собирается в целях управления лицензиями и оценки параметров работы устройства и потоков обрабатываемых им данных. Это позволяет контролировать общее состояние и параметры подключения к маршрутизатору, устранять возникающие ошибки, анализировать использование продуктов и реагировать на предупредительные сообщения.</p> <p>3. Сведения об использовании устройства обрабатываются в следующих целях:</p> <ul style="list-style-type: none"> <li>• оптимизация параметров работы Norton Core;</li> <li>• информирование пользователей о безопасности той или иной площадки; и</li> <li>• блокировка доступа к небезопасным веб-сайтам.</li> </ul> <p>4. Данные и настройки родительского контроля используются для контроля соблюдения политик и правил, выбранных пользователем в отношении контролируемых профилей, оказания пользователю содействия в выявлении случаев несанкционированного использования Персональных данных, связанных с такими профилями, и взаимодействия с пользователем и контролируемыми профилями.</p> <p>5.-6. Данные об учетной записи пользователя собираются Symantec для оказания услуг, указанных в договоре с покупателем, включая необходимое содействие и услуги технической поддержки.</p> <p>7. Телеметрические данные по киберугрозам передаются Symantec для проведения исследований и разработок в целях усовершенствования продуктов и сервисов Symantec и оптимальной защиты сети, устройств, информации и идентификационных данных пользователя.</p> <p>8. Контактные данные и информация о предпочтениях пользователя передаются Symantec в следующих целях:</p> <ul style="list-style-type: none"> <li>• оказание пользователю содействия при установке Norton Core;</li> <li>• информирование пользователя о возможностях продукта или сервиса;</li> <li>• предоставление пользователю адаптированной информации исходя из заданных предпочтений (включая язык и место нахождения); и</li> <li>• повышение удовлетворенности пользователей качеством обслуживания за счет использования своих собственных или сторонних контакт-центров.</li> </ul> <p>9. Адрес доставки и связанная с ним информация требуются для доставки пользователю аппаратных средств Norton Core.</p> <p>10. Для получения информации о Norton Community Watch см. раздел «Norton Community Watch» настоящего Уведомления.</p> <p>Кроме того, Symantec использует полученную информацию для создания агрегированных, обезличенных и иным образом обработанных данных, которые не позволяют установить конкретное устройство или пользователя, включая статистическую информацию, в следующих целях:</p> <ul style="list-style-type: none"> <li>• проведение исследований в области кибербезопасности;</li> </ul>

	<p>7. Телеметрические данные по киберугрозам, включая журналы регистрации попыток загрузить вредоносные исполняемые файлы (мобильные приложения), сведения о других сомнительных событиях и действиях и сами программные продукты (в том числе образцы вредоносного ПО)</p> <p>*8. Контактные данные пользователя и заданные предпочтения</p> <p>*9. Адрес доставки и связанная с этим информация</p> <p>10. Norton Core позволяет стать участником программы Norton Community Watch</p>	<ul style="list-style-type: none"> <li>• расширение возможностей для выявления вредоносного ПО и киберугроз, в том числе за счет анализа выборочных данных;</li> <li>• отслеживание и публикация отчетов о тенденциях и рисках в области безопасности (включая кражу персональных данных);</li> <li>• проведение статистического анализа применительно к используемым продуктам, включая оценку тенденций и сравнение с данными в базе агрегированных данных пользователей;</li> <li>• контроль и усовершенствование параметров работы продуктов с точки зрения их доступности и времени реагирования;</li> <li>• оценка частоты обращений пользователей для получения информации о продуктах в целях повышения эффективности использования продуктов; и</li> <li>• получение других обезличенных аналитических данных для оценки конъюнктуры рынка и коммерческих возможностей и повышения эффективности работы компании.</li> </ul>
--	--	---

## Norton Mobile Security

Описание Продукта или Сервиса	Условия доступа и сбора данных	Обработка информации
<p>Norton Mobile Security обеспечивает защиту смартфонов и планшетных устройств пользователей, которые были подписаны абонентом на сервис, от цифровых угроз и возможность восстановления данных (включая контактную информацию) в случае утери или кражи устройства.</p>	<p>1. Данные о мобильных устройствах подписанных на сервис пользователей, включая идентификационные номера аппаратных средств (IMEI, MAC-адрес WiFi, UDID и т.п.), информацию об абоненте, номер мобильного телефона и другую контактную информацию подписанных на сервис пользователей, название или тип устройства и его производителя, тип и версию операционной системы, оператора беспроводной связи, тип сети, страну происхождения, идентификационный номер дела в службе поддержки, установленные пользователем сертификаты, доменное имя веб-сайта и связанную с ним цепочку SSL-сертификатов от устройства и IP-адрес</p> <p>2. Данные об использовании, включая сведения о частоте загрузки и использования, зарегистрированные данные и cookie-файлы и информацию о</p>	<p>1. Данные о мобильных устройствах и абоненте и контактная информация подключенных к сервису пользователей обрабатываются в следующих целях:</p> <ul style="list-style-type: none"> <li>• обеспечение работоспособности и повышение эффективности работы Продукта;</li> <li>• подтверждение Symantec идентификационных данных подключенных к сервису пользователей;</li> <li>• оказание пользователю содействия при установке программного обеспечения;</li> <li>• взаимодействие с подключенными к сервису пользователями для оказания соответствующих услуг;</li> <li>• управление лицензиями; и</li> <li>• повышение удовлетворенности пользователей качеством обслуживания за счет использования своих собственных или сторонних контакт-центров.</li> </ul> <p>2. Сведения об использовании устройства обрабатываются в следующих целях: оценка параметров использования продукта и предпочтений пользователей в целях индивидуализации оказываемых услуг и повышения эффективности работы с продуктом.</p> <p>3. Имена файлов и приложений, данные календаря (включая приглашительные ссылки) и информация, сохраненная на карте памяти, обрабатываются в следующих целях:</p> <ul style="list-style-type: none"> <li>• предупреждение пользователя о потенциально опасных приложениях;</li> <li>• сканирование устройства для выявления вредоносного ПО; и</li> <li>• удаление персональных данных с устройства пользователя (при условии, что на Продукте будет включена и активирована функция Wipe).</li> </ul> <p>4. Данные о просмотренных страницах в сети Интернет обрабатываются в следующих целях:</p>

<p>сетевых службах (как пользователь подключается к сетевым службам)</p> <p>3. Имена файлов и приложений на пользовательском устройстве, считываемые при очередном сканировании, выполняемом соответствующим Продуктом, включая отсканированные приложения, которые на данный момент не включены в базу данных Symantec и не отнесены к категории известных приложений, для защиты пользователя от вредоносного ПО и непроверенных функций, в том числе данные календаря и информация, сохраненная на карте памяти (если применимо)</p> <p>4. Адреса просмотренных веб-сайтов, журналы просмотра и закладки</p> <p>*5. Контакты на устройстве пользователя (на усмотрение пользователя), включая зарегистрированные звонки и текстовые сообщения</p> <p>6. Настройки телефонных звонков и звука</p> <p>*7. Данные о месте нахождения устройства</p> <p>*8. Продукт также может быть настроен таким образом, чтобы (при наличии такой возможности) в случае кражи или утери устройства и дальнейшего использования устройства, ввода неверного пароля после одной неудачной попытки разблокировать устройство или включения устройства после выключения фронтальная камера фотографировала пользователя устройства</p> <p>9. Резервное копирование сохраненных на мобильном устройстве данных, включая контакты, журнал звонков, номера телефонов и текстовые сообщения</p>	<ul style="list-style-type: none"> <li>• информирование пользователей о безопасности той или иной площадки;</li> <li>• блокировка доступа к небезопасным веб-сайтам; и</li> <li>• очистка журнала посещений и удаление закладок (при условии что на Продукте будет включена функция Web Protection или Wipe).</li> </ul> <p>5. Сведения о контактах (включая журналы звонков и текстовые сообщения), сохраненные на устройстве пользователя, обрабатываются в целях блокировки вызовов и текстовых сообщений (на усмотрение пользователя).</p> <p>6. Настройки телефона используются для блокировки входящих вызовов от сохраненных контактов и внесения изменений в настройки звука на устройстве, при условии что пользователь активирует поддерживаемую Продуктом функцию блокировки и (или) использует команду Scream.</p> <p>7. 8. Сведения о месте нахождения устройства и изображения могут быть получены по запросу подключенного к сервису пользователя для обнаружения устройства в случае его кражи или утери. Кроме того, абонент может воспользоваться функцией дистанционного управления для поиска устройства подключенного к сервису пользователя в случае его кражи или утери. При определенных обстоятельствах после получения информации о краже или утере устройство будет заблокировано дистанционно. Также в этом случае устройство может быть в любое время выключено. С согласия подключенного к сервису пользователя может также сохраняться информация о последнем местонахождении устройства (до 10 мест), с тем чтобы пользователь мог отслеживать его перемещения, даже если продукт в настоящее время не используется.</p> <p>9. Резервные данные обрабатываются в целях использования поддерживаемых Продуктом функций резервного копирования и восстановления (если эти функции используются пользователем).</p> <p>Кроме того, Symantec использует полученную информацию для создания агрегированных, обезличенных и иным образом обработанных данных, которые не позволяют установить конкретное устройство или пользователя, включая статистическую информацию, в следующих целях:</p> <ul style="list-style-type: none"> <li>• проведение исследований в области кибербезопасности;</li> <li>• расширение возможностей для выявления вредоносного ПО и киберугроз, в том числе за счет анализа выборочных данных;</li> <li>• отслеживание и публикация отчетов о тенденциях и рисках в области безопасности (включая кражу персональных данных);</li> <li>• проведение статистического анализа применительно к используемым продуктам, включая оценку тенденций и сравнение с данными в базе агрегированных данных пользователей;</li> <li>• контроль и усовершенствование параметров работы продуктов с точки зрения их доступности и времени реагирования;</li> <li>• оценка частоты обращений пользователей для получения информации о продуктах в целях повышения эффективности использования продуктов; и</li> <li>• получение других обезличенных аналитических данных для оценки конъюнктуры рынка и коммерческих возможностей и повышения эффективности работы компании.</li> </ul>
--	---

## Norton Security Scan

Описание Продукта или Сервиса	Условия доступа и сбора данных	Обработка информации
<p>Norton Secure Scan сканирует конечное устройство или устройства, указанные пользователем, выявляет возможные проблемы или опасности и дает рекомендации по использованию тех или иных продуктов и решений.</p>	<p>1. Идентификатор машины (данные, генерируемые Symantec); поддерживаемая устройством функция установки и удаления программ; данные об устройстве; сведения о пользовательском посреднике устройства (приложения), включая тип устройства, версию и язык операционной системы, производитель и модель; операционная система; и информация о местоположении устройства</p> <p>2. Телеметрические данные о просканированных файлах, особенностях использования продукта или сервиса пользователем и выявленных, ликвидированных и оставшихся угрозах; дата и время сканирования после запуска; сведения о состоянии (установка и работа), которые также могут включать персональные данные, указанные в пути к файлу или имени папки</p>	<p>1. Идентификатор машины и связанная с ним информация используется Symantec в следующих целях:</p> <ul style="list-style-type: none"> <li>оказание пользователю содействия при установке программного обеспечения;</li> <li>взаимодействие с пользователями для оказания соответствующих услуг;</li> <li>оценка параметров использования сервиса и предпочтений пользователей в целях индивидуализации оказываемых услуг и повышения эффективности работы с продуктом.</li> </ul> <p>2. Телеметрические данные используются Symantec в следующих целях:</p> <ul style="list-style-type: none"> <li>обеспечение работоспособности и повышение эффективности работы Сервиса; и</li> <li>проведение исследований и разработок в целях усовершенствования продуктов и сервисов Symantec и оптимальной защиты сети, устройств, информации и идентификационных данных пользователя.</li> </ul> <p>Кроме того, Symantec использует полученную информацию для создания агрегированных, обезличенных и иным образом обработанных данных, которые не позволяют установить конкретное устройство или пользователя, включая статистическую информацию, в следующих целях:</p> <ul style="list-style-type: none"> <li>проведение исследований в области кибербезопасности;</li> <li>расширение возможностей для выявления вредоносного ПО и киберугроз, в том числе за счет анализа выборочных данных;</li> <li>отслеживание и публикация отчетов о тенденциях и рисках в области безопасности (включая кражу персональных данных);</li> <li>проведение статистического анализа применительно к используемым продуктам, включая оценку тенденций и сравнение с данными в базе агрегированных данных пользователей;</li> <li>контроль и усовершенствование параметров работы продуктов с точки зрения их доступности и времени реагирования;</li> <li>оценка частоты обращений пользователей для получения информации о продуктах в целях повышения эффективности использования продуктов; и</li> <li>получение других обезличенных аналитических данных для оценки конъюнктуры рынка и коммерческих возможностей и повышения эффективности работы компании.</li> </ul>



## Norton Secure Login

Описание Продукта или Сервиса	Условия доступа и сбора данных	Обработка информации
<p>Norton Secure Login (NSL) — поставщик идентификационной информации, обеспечивающий простой, безопасный и централизованный способ аутентификации пользователей. Symantec предоставляет инфраструктуру для управления идентификацией миллионов пользователей многочисленных продуктов Norton.</p>	<p>*1. Персональные данные, которые позволяют установить личность пользователя, включая домашний адрес, номер телефона, дату рождения и (или) номер банковской карты; контактная информация пользователя; любые другие Персональные данные, указываемые пользователем в Учетной записи Norton или предоставляемые в целях оказания услуг поддержки и содействия при подключении (включая ФИО и сведения об устройстве)</p> <p>2. Сведения об устройстве, продукте и сервисе; сведения о пользовательском посреднике устройства (приложения), включая тип устройства, тип и версию операционной системы, производителя и модель; сведения об устройстве и пользовательском посреднике устройства (приложения), включая тип устройства, тип и версию операционной системы, производителя и модель; данные о производительности, установленных приложениях и местоположении; MAC-адрес и IP-адрес</p> <p>3. Данные о пользовании Интернетом, включая адреса и IP-адреса открываемых веб-сайтов, ключевые слова и результаты поиска; сведения о потенциальных угрозах безопасности (включая адреса и IP-адреса веб-сайтов, которые были отнесены к категории подозрительных и мошеннических веб-сайтов, где могут содержаться Персональные данные, которые веб-сайт пытается получить без разрешения пользователя)</p>	<p>1. Персональные данные используются Symantec в следующих целях:</p> <ul style="list-style-type: none"> <li>установление личности пользователя в интересах Symantec или связанных с ней третьих лиц, которые используют Norton Security Login;</li> <li>подтверждение аутентификации и (или) предотвращение мошеннических действий, которые могут совершаться от имени пользователя;</li> <li>оказание пользователю содействия при настройке;</li> <li>взаимодействие с пользователем для оказания услуг, включая услуги поддержки и содействия; и</li> <li>повышение удовлетворенности пользователей качеством обслуживания за счет использования своих собственных или сторонних контакт-центров.</li> </ul> <p>2. Информация об устройстве, продуктах и сервисах используется Symantec в следующих целях:</p> <ul style="list-style-type: none"> <li>обеспечение работоспособности и повышение эффективности работы Продуктов и Сервисов;</li> <li>управление лицензиями; и</li> <li>оценка параметров использования продукта и предпочтений пользователей в целях индивидуализации оказываемых услуг и повышения эффективности работы с продуктом.</li> </ul> <p>3. Данные об использовании обрабатываются Symantec в следующих целях:</p> <ul style="list-style-type: none"> <li>информирование пользователей о безопасности той или иной площадки;</li> <li>блокировка доступа к небезопасным веб-сайтам; и</li> <li>проведение исследований и разработок в целях усовершенствования продуктов и сервисов Symantec и оптимальной защиты сети, устройств, информации и идентификационных данных пользователя.</li> </ul> <p>Кроме того, Symantec использует полученную информацию для создания агрегированных, обезличенных и иным образом обработанных данных, которые не позволяют установить конкретное устройство или пользователя, включая статистическую информацию, в следующих целях:</p> <ul style="list-style-type: none"> <li>проведение исследований в области кибербезопасности;</li> <li>расширение возможностей для выявления вредоносного ПО и киберугроз, в том числе за счет анализа выборочных данных;</li> <li>отслеживание и публикация отчетов о тенденциях и рисках в области безопасности (включая кражу персональных данных);</li> <li>проведение статистического анализа применительно к используемым продуктам, включая оценку тенденций и сравнение с данными в базе агрегированных данных пользователей;</li> <li>контроль и усовершенствование параметров работы продуктов с точки зрения их доступности и времени реагирования;</li> <li>оценка частоты обращений пользователей для получения информации о продуктах в целях повышения эффективности использования продуктов; и</li> <li>получение других обезличенных аналитических данных для оценки конъюнктуры рынка и коммерческих возможностей и повышения эффективности работы компании.</li> </ul>

## Norton Ultimate Help-Desk и Norton Computer Tune-Up

Описание Продукта или Сервиса	Условия доступа и сбора данных	Обработка информации
<p>Norton Ultimate Help Desk позволяет пользователю связываться со специалистом, который может оказать содействие в решении технических вопросов, включая настройки сети и диагностику и устранение неполадок в работе устройства.</p> <p>Norton Computer Tune-Up — одна из функций Norton Ultimate Help Desk, призванная через диагностику устройства пользователя обеспечить его бесперебойную работу с характеристиками, сопоставимыми с параметрами работы нового устройства.</p>	<p>*1. Сведения, указываемые вами при обращении в службу поддержки Symantec по телефону или указываемые в специальной форме на сайте Symantec при оформлении заявки на доступ к Сервисам Norton</p> <p>2. Информация о системе, включая: тип и версию операционной системы и используемого на устройстве браузера; сведения о наличии работающего экрана межсетевой защиты; информацию об установленном, работающем и обновленном антивирусном ПО; данные об объеме памяти и дискового пространства и настройках прокси-сервера; перечни файлов каталога для Support Software Tool; сведения о веб-браузере, включая настройки безопасности и хранения временных файлов; активные порты, файлы узла и заданные на устройстве настройки сетевого интерфейса; сведения об установленных программах и активных процессах; журналы регистрации событий приложений и операционной системы и данные системного реестра</p> <p>3. Диагностическая информация, включая: количество просканированных файлов, обнаруженных и ликвидированных Support Software Tool угроз; типы обнаруженных угроз; состояние системы безопасности (хорошее, удовлетворительное или неудовлетворительное) устройства по оценке Support Software Tool; количество и типы угроз, которые не были ликвидированы Support Software Tool</p>	<p>1. Данные, указываемые пользователем при обращении в службу поддержки, обрабатываются Symantec в следующих целях:</p> <ul style="list-style-type: none"> <li>• взаимодействие с пользователями для оказания соответствующих услуг;</li> <li>• оценка параметров использования продукта и предпочтений пользователей в целях индивидуализации оказываемых услуг и повышения эффективности работы с продуктом; и</li> <li>• повышение удовлетворенности пользователей качеством обслуживания за счет использования своих собственных или сторонних контакт-центров.</li> </ul> <p>2. Информация о системе обрабатывается Symantec в следующих целях:</p> <ul style="list-style-type: none"> <li>• предоставление пользователю доступа к запрашиваемым Сервисам;</li> <li>• обеспечение работоспособности и повышение эффективности работы Сервисов; и</li> <li>• оказание пользователю содействия при использовании Сервисов.</li> </ul> <p>3. Диагностическая информация обрабатывается Symantec в следующих целях:</p> <ul style="list-style-type: none"> <li>• информирование пользователя о результатах оказания услуг; и</li> <li>• проведение исследований и разработок в целях усовершенствования продуктов и сервисов Symantec и оптимальной защиты сети, устройств, информации и идентификационных данных пользователя.</li> </ul> <p>Кроме того, Symantec использует полученную информацию для создания агрегированных, обезличенных и иным образом обработанных данных, которые не позволяют установить конкретное устройство или пользователя, включая статистическую информацию, в следующих целях:</p> <ul style="list-style-type: none"> <li>• проведение исследований в области кибербезопасности;</li> <li>• расширение возможностей для выявления вредоносного ПО и киберугроз, в том числе за счет анализа выборочных данных;</li> <li>• отслеживание и публикация отчетов о тенденциях и рисках в области безопасности (включая кражу персональных данных);</li> <li>• проведение статистического анализа применительно к используемым продуктам, включая оценку тенденций и сравнение с данными в базе агрегированных данных пользователей;</li> <li>• контроль и усовершенствование параметров работы продуктов с точки зрения их доступности и времени реагирования;</li> <li>• оценка частоты обращений пользователей для получения информации о продуктах в целях повышения эффективности использования продуктов; и</li> <li>• получение других обезличенных аналитических данных для оценки конъюнктуры рынка и коммерческих возможностей и повышения эффективности работы компании.</li> </ul>

## Norton Secure VPN (раньше Norton WiFi Privacy)

Описание Продукта или Сервиса	Условия доступа и сбора данных	Обработка информации
<p>Norton Secure VPN защищает устройства и данные пользователя путем шифрования соответствующей информации при подключении к Интернету, что гарантирует конфиденциальность данных пользователя.</p>	<p>1. Сведения об абоненте и мобильном устройстве, включая название устройства, тип, язык и версию операционной системы</p> <p>2. Коэффициент использования совокупной пропускной способности</p> <p>3. Сведения о временном использовании, которые помогают устранять выявляемые сбои в работе сервисов.</p>	<p>1. Сведения об абоненте и мобильном устройстве обрабатываются Symantec в следующих целях:</p> <ul style="list-style-type: none"> <li>• обеспечение работоспособности и повышение эффективности работы Сервисов;</li> <li>• оценка параметров использования продукта и предпочтений пользователей в целях индивидуализации оказываемых услуг и повышения эффективности работы с продуктом;</li> <li>• оказание пользователю содействия при установке ПО и пользовании Сервисами;</li> <li>• взаимодействие с пользователями для оказания соответствующих услуг;</li> <li>• уведомление пользователя о необходимости обеспечить защиту передаваемой информации; и</li> <li>• повышение удовлетворенности пользователей качеством обслуживания за счет использования своих собственных или сторонних контакт-центров.</li> </ul> <p>2. Коэффициент использования совокупной пропускной способности требуется Symantec для выставления счетов, оказания услуг поддержки и обслуживания сети.</p> <p>3. Данные о временном использовании обрабатываются Symantec в следующих целях:</p> <ul style="list-style-type: none"> <li>• выбор наиболее подходящего сервера для подключения; и</li> <li>• проведение исследований и разработок в целях усовершенствования продуктов и сервисов Symantec и оптимальной защиты сети, устройств, информации и идентификационных данных пользователя.</li> </ul> <p>При использовании Norton Secure VPN мы пропускаем Интернет-трафик через сеть Symantec, где журналы регистрации не ведутся. Это означает, что при подключении к Norton Secure VPN Symantec не сохраняет IP-адрес пользователя, передающего те или иные данные; таким образом, Symantec не может установить личность пользователя. Автоматизированная система управления трафиком Symantec на основе правил может предусматривать анализ данных, передаваемых в сети Интернет, в режиме реального времени, включая целевые веб-сайты, IP-адрес отправителя и получателя; при этом журналы для регистрации этой информации не ведутся. Symantec не хранит информацию о приложениях, сервисах и веб-сайтах, загружаемых, используемых или посещаемых пользователем. Поскольку Symantec управляет глобальной сетью, Интернет-трафик пользователя может проходить через одну или несколько стран (см. <a href="#">Глобальное заявление Symantec-Norton о конфиденциальности</a>).</p> <p>Кроме того, Symantec использует полученную информацию для создания агрегированных, обезличенных и иным образом обработанных данных, которые не позволяют установить конкретное устройство или пользователя, включая статистическую информацию, в следующих целях:</p> <ul style="list-style-type: none"> <li>• проведение исследований в области кибербезопасности;</li> <li>• расширение возможностей для выявления вредоносного ПО и киберугроз, в том числе за счет анализа выборочных данных;</li> <li>• отслеживание и публикация отчетов о тенденциях и рисках в области безопасности (включая кражу персональных данных);</li> <li>• проведение статистического анализа применительно к используемым продуктам, включая оценку тенденций и сравнение с данными в базе агрегированных данных пользователей;</li> <li>• контроль и усовершенствование параметров работы продуктов с точки зрения их доступности и времени реагирования;</li> <li>• оценка частоты обращений пользователей для получения информации о продуктах в целях повышения эффективности использования продуктов; и</li> <li>• получение других обезличенных аналитических данных для оценки конъюнктуры рынка и коммерческих возможностей и повышения эффективности работы компании.</li> </ul>

## Средства обеспечения безопасности Norton (Security, Internet Security, One, Antivirus и 360)

В настоящем разделе приведено описание Norton Security (версии Standard, Deluxe и Premium), Norton Internet Security, Norton One, Norton Antivirus, Norton Antivirus Basic, Norton 360, Norton 360PE и Norton 360MD.

Описание Продукта или Сервиса	Условия доступа и сбора данных	Обработка информации
<p>Средства безопасности Norton обеспечивают безопасность конечных устройств и защищают их от программ-вымогателей, вирусов, шпионского и вредоносного ПО и других угроз в сети Интернет.</p>	<p>1. Сведения об абоненте и устройстве, включая</p> <ul style="list-style-type: none"> <li>*Персональные данные, которые указывает пользователь при создании Учетной записи Norton, в том числе имя пользователя и графическое изображение (аватар);</li> <li>*Персональные данные, указываемые пользователем при задании имени устройства; ФИО или имя-псевдоним лица, которому передано устройство (при условии что эти данные указаны пользователем); сведения о пользовательском посреднике устройства (приложения), включая тип, производителя и модель устройства, тип и версию операционной системы; виды и версии приложений; данные о местонахождении; MAC-адрес; идентификатор машины и IP-адрес; сведения о состоянии при установке и работе, которые могут включать Персональные данные, указываемые в имени файла или папки; дополнительные Персональные данные, предоставляемые пользователем Symantec для оказания услуг поддержки и содействия при подключении (идентификатор и имя пользователя; сведения о правах и полномочиях, политиках и устройстве)</li> </ul> <p>2. Данные о пользовании Интернетом, включая адреса и IP-адреса открываемых веб-сайтов, ключевые слова и результаты поиска; сведения о потенциальных угрозах безопасности (включая адреса и IP-адреса веб-сайтов, которые были отнесены к категории подозрительных и мошеннических веб-сайтов, где могут содержаться Персональные данные, которые веб-сайт пытается получить без разрешения пользователя)</p> <p>3. Данные об использовании и результатах диагностики устройства, включая: информацию о том, когда устройство использовалось в последний раз, и времени пользования Интернетом по каждому подключенному устройству; протоколы шлюзов с указанием подключений к сети; исполняемые файлы, отнесенные к категории потенциально опасных, которые могут включать Персональные данные, доступ к которым получен вредоносным ПО без разрешения пользователя; сообщения электронной почты, отправляемые Symantec с разрешения пользователя и отнесенные к категории</p>	<p>1. Сведения об абоненте и устройстве обрабатываются Symantec в следующих целях:</p> <ul style="list-style-type: none"> <li>• обеспечение работоспособности и повышение эффективности работы Продуктов и Сервисов;</li> <li>• подтверждение Symantec идентификационных данных пользователей;</li> <li>• оценка параметров использования продукта и предпочтений пользователей в целях индивидуализации оказываемых услуг и повышения эффективности работы с продуктом;</li> <li>• оказание пользователю содействия при установке программного обеспечения;</li> <li>• взаимодействие с пользователями для оказания соответствующих услуг;</li> <li>• управление лицензиями; и</li> <li>• повышение удовлетворенности пользователей качеством обслуживания за счет использования своих собственных или сторонних контакт-центров.</li> </ul> <p>2. Сведения о пользовании Интернетом обрабатываются в следующих целях:</p> <ul style="list-style-type: none"> <li>• информирование пользователя о безопасности той или иной площадки; и</li> <li>• блокировка доступа к небезопасным веб-сайтам.</li> </ul> <p>3. Данные об устройстве и результатах диагностики обрабатываются Symantec в следующих целях:</p> <ul style="list-style-type: none"> <li>• оценка использования продукта;</li> <li>• обеспечение работоспособности функций защиты, поддерживаемых Продуктами и Сервисами; и</li> <li>• проведение исследований и разработок в целях усовершенствования продуктов и сервисов Symantec и оптимальной защиты сети, устройств, информации и идентификационных данных пользователя.</li> </ul> <p>4. Данные и настройки родительского контроля используются для контроля соблюдения политик и правил, заданных пользователем в отношении контролируемых профилей, оказания пользователю содействия в выявлении случаев несанкционированного использования Персональных данных, связанных с такими профилями, и взаимодействия с пользователем и контролируруемыми профилями.</p> <p>Кроме того, Symantec использует полученную информацию для создания агрегированных, обезличенных и иным образом обработанных данных, которые не позволяют установить конкретное устройство или пользователя, включая статистическую информацию, в следующих целях:</p> <ul style="list-style-type: none"> <li>• проведение исследований в области кибербезопасности;</li> <li>• расширение возможностей для выявления вредоносного ПО и киберугроз, в том числе за счет анализа выборочных данных;</li> </ul>

	<p>нежелательных сообщений (в том числе необоснованно); данные о состоянии на момент сбоя или сведения, приведенные в отчете, который отправляется Symantec в соответствии с заданными пользователем настройками при обнаружении ошибок или сбоев в работе Продуктов и Сервисов, включая язык и тип операционной системы, страну местонахождения, процессы или файлы, исполняемые в момент обнаружения ошибки</p> <p>4. Данные и настройки родительского контроля, заданные пользователем, включая заблокированные веб-сайты, посещенные веб-сайты, сведения о фильтрации по времени и содержанию и адреса веб-сайтов, которые представляют или могут представлять опасность</p>	<ul style="list-style-type: none"> <li>• отслеживание и публикация отчетов о тенденциях и рисках в области безопасности (включая кражу персональных данных);</li> <li>• проведение статистического анализа применительно к используемым продуктам, включая оценку тенденций и сравнение с данными в базе агрегированных данных пользователей;</li> <li>• контроль и усовершенствование параметров работы продуктов с точки зрения их доступности и времени реагирования;</li> <li>• оценка частоты обращений пользователей для получения информации о продуктах в целях повышения эффективности использования продуктов; и</li> <li>• получение других обезличенных аналитических данных для оценки конъюнктуры рынка и коммерческих возможностей и повышения эффективности работы компании.</li> </ul>
--	--	---

## Norton Safe Search, Norton Home Page, Norton Safe Web

Описание Продукта или Сервиса	Условия доступа и сбора данных	Обработка информации
<p>Norton Safe Search — поисковая служба, которая помогает защитить пользователя от небезопасных веб-сайтов путем фильтрации результатов поиска и присвоения веб-сайтам рейтинга с точки зрения их безопасности, что повышает уровень безопасности при посещении пользователем различных веб-сайтов. Кроме того, данный сервис представляет собой одно из расширений веб-браузера, обеспечивающее доступ к веб-сайту Norton Safe Search разными способами. Разные версии этого расширения на усмотрение пользователя способны:</p> <p>а) использовать вместо поисковой службы браузера, заданной по</p>	<p>1. Сведения об абоненте, устройстве и ПО, включая: название, версию и предпочтительный язык веб-браузера; тип или версию операционной системы; IP-адрес пользовательского устройства</p> <p>2. Данные об использовании сервиса, включая: ссылки в социальных сетях и веб-почте; сведения о посещаемых веб-сайтах; ключевые слова, используемые для поиска; информацию, заданную по умолчанию в различных окнах поиска, управляемых продуктами Norton; результаты поиска</p> <p>3. Cookie-файлы; пиксельные теги; сценарии и другие</p>	<p>1. Сведения об абоненте, устройстве и ПО обрабатываются Symantec в следующих целях:</p> <ul style="list-style-type: none"> <li>• обеспечение работоспособности и повышение эффективности работы Сервисов;</li> <li>• управление лицензиями;</li> <li>• оценка параметров использования продукта и предпочтений пользователей в целях индивидуализации оказываемых услуг и повышения эффективности работы с продуктом;</li> <li>• оказание пользователю содействия при установке программного обеспечения;</li> <li>• совершенствование Продуктов и Сервисов, повышение степени защиты пользователя, сети, устройства, данных и личности пользователя; и</li> <li>• повышение удовлетворенности пользователей качеством обслуживания за счет использования своих собственных или сторонних контакт-центров.</li> </ul> <p>2. Данные об использовании Сервиса обрабатываются Symantec и уполномоченными ею лицами в следующих целях:</p> <ul style="list-style-type: none"> <li>• информирование пользователя о безопасности той или иной площадки;</li> <li>• блокировка доступа к небезопасным веб-сайтам; и</li> <li>• анализ использования Сервиса.</li> </ul> <p>Все поисковые запросы, формируемые пользователем через Norton Safe Search, переадресуются на сайты сторонних поставщиков и наших партнеров Oath/Yahoo! (для пользователей из США и Канады) и IACI (для пользователей из других стран) для поиска и предоставления вам запрашиваемой информации. Наши сторонние поставщики и партнеры могут также получать информацию непосредственно от вас при использовании вами Norton Safe Search. В этом случае наши сторонние поставщики и партнеры действуют в качестве операторов персональных данных в целях обработки ваших запросов. В этом случае сбор данных регулируется Политикой, Заявлением и Уведомлением о конфиденциальности сторонних поставщиков и партнеров.</p> <p>При использовании Norton Safe Search ваш запрос переадресовывается стороннему поставщику и партнеру (т.е. компании, не связанной с Symantec), который и обрабатывает полученный запрос. Наши сторонние поставщики и</p>

<p>умолчанию, Norton Safe Search; или</p> <p>b) использовать вместо поисковой службы браузера, заданной по умолчанию, Norton Safe Search И одновременно заменять домашнюю страницу браузера по умолчанию на Norton Home Page + вводить новые настройки для вкладок.</p> <p>Norton Home Page — расширение браузера и домашняя страница по умолчанию со встроенной поисковой системой Norton Safe Search.</p> <p>Norton Safe Web — расширение браузера, используемое пользователем для контроля действий в сети Интернет и содержания веб-страниц. Данный сервис оценивает репутацию и содержание веб-страницы и помогает защитить пользователя от вредоносного содержания веб-сайтов, фишинга и других угроз.</p>	<p>подобные технологии, размещаемые Norton Safe Search и Norton Home Page на ПК или устройстве</p>	<p>партнеры могут также получать информацию непосредственно от вас при использовании вами Norton Safe Search (в дальнейшем собирательно именуется «Данные, собираемые сторонними поставщиками»). Сторонние поставщики и партнеры при обработке ваших запросов выступают в роли операторов персональных данных. Таким образом, именно сторонний поставщик и партнер, а не Symantec, принимает решение о том, как именно будут собираться, использоваться, передаваться, храниться и обрабатываться иным образом Данные, собираемые сторонними поставщиками. При обработке вашей информации и поисковых запросов данные, собираемые сторонними поставщиками, регулируются заявлением(-ями) о конфиденциальности таких сторонних поставщиков и партнеров. См. заявления о конфиденциальности <a href="#">сторонних партнеров</a>.</p> <p>3. Cookie-файлы и другие подобные средства отслеживания обрабатываются для учета предпочтений пользователя при использовании теми или иными функциями и параметров их использования в прошлом. Для получения подробной информации о cookie-файлах см. раздел «Технологии отслеживания, cookie-файлы и команды на запрет отслеживания» в <a href="#">Глобальном заявлении Symantec-Norton о конфиденциальности</a>.</p> <p><a href="#">Обезличенные IP-адреса</a> и данные об использовании продуктов обрабатываются Протоколом передачи статистических данных (Measurement Protocol) <a href="#">Google Analytics</a> для статистического анализа и управления критическими ошибками. Для получения дополнительной информации см. <a href="#">информацию о средствах защиты данных Google Analytics</a>.</p> <p>Кроме того, Symantec использует полученную информацию для создания агрегированных, обезличенных и иным образом обработанных данных, которые не позволяют установить конкретное устройство или пользователя, включая статистическую информацию, в следующих целях:</p> <ul style="list-style-type: none"><li>• проведение исследований в области кибербезопасности;</li><li>• расширение возможностей для выявления вредоносного ПО и киберугроз, в том числе за счет анализа выборочных данных;</li><li>• отслеживание и публикация отчетов о тенденциях и рисках в области безопасности (включая кражу персональных данных);</li><li>• проведение статистического анализа применительно к используемым продуктам, включая оценку тенденций и сравнение с данными в базе агрегированных данных пользователей; и</li><li>• контроль и усовершенствование параметров работы продуктов с точки зрения их доступности и времени реагирования.</li></ul>
--	--	---

## Norton Security Toolbar

Описание Продукта или Сервиса	Условия доступа и сбора данных	Обработка информации
<p>Norton Security Toolbar может использоваться двумя способами: а) в виде расширения Microsoft Internet Explorer; и б) в виде расширения Google Chrome. В обоих случаях Norton Security Toolbar используется для контроля действий пользователя в сети Интернет и содержания веб-сайтов. Данный сервис оценивает репутацию и содержание веб-страницы и помогает защитить пользователя от вредоносного содержания веб-сайтов, фишинга и других угроз.</p> <p>В случае использования Norton Security Toolbar в виде расширения Internet Explorer пользователь получает доступ и может использовать сохраненные данные Norton Identity Safe в пользовательском интерфейсе браузера. Кроме того, доступно окно поиска для пользования службой Norton Safe Search. В случае использования Norton Security Toolbar в виде расширения Google Chrome доступно окно поиска для пользования службой Norton Safe Search.</p>	<p>1. Данные об устройстве и ПО, включая: название, версию и предпочтительный язык веб-браузера; тип или версию операционной системы; IP-адрес пользовательского устройства</p> <p>2. Данные об использовании Продукта, включая: сведения о посещаемых веб-сайтах (включая сокращенную версию такой информации); ключевые слова, используемые для поиска; информацию, заданную по умолчанию в различных окнах поиска, управляемых продуктами Norton; результаты поиска</p> <p>3. Cookie-файлы; пиксельные теги; сценарии и другие подобные технологии, размещаемые Norton Safe Search и Norton Home Page на ПК или устройстве</p>	<p>1. Данные об устройстве и ПО обрабатываются Symantec в следующих целях:</p> <ul style="list-style-type: none"> <li>• обеспечение работоспособности и повышение эффективности работы Сервисов;</li> <li>• управление лицензиями;</li> <li>• оценка параметров использования продукта и предпочтений пользователей в целях индивидуализации оказываемых услуг и повышения эффективности работы с продуктом;</li> <li>• оказание пользователю содействия при установке программного обеспечения;</li> <li>• совершенствование Продуктов и Сервисов, повышение степени защиты пользователя, сети, устройства, данных и личности пользователя; и</li> <li>• повышение удовлетворенности пользователей качеством обслуживания за счет использования своих собственных или сторонних контакт-центров.</li> </ul> <p>2. Данные об использовании Продукта обрабатываются Symantec и уполномоченными ею лицами в следующих целях:</p> <ul style="list-style-type: none"> <li>• информирование пользователя о безопасности той или иной площадки;</li> <li>• блокировка доступа к небезопасным веб-сайтам; и</li> <li>• анализ использования Сервиса.</li> </ul> <p>3. Cookie-файлы и другие подобные средства отслеживания обрабатываются для учета предпочтений пользователя при пользовании теми или иными функциями и параметров их использования в прошлом. Для получения подробной информации о cookie-файлах см. раздел «Технологии отслеживания, cookie-файлы и команды на запрет отслеживания» в <a href="#">Глобальном заявлении Symantec-Norton о конфиденциальности</a>.</p> <p>Кроме того, Symantec использует полученную информацию для создания агрегированных, обезличенных и иным образом обработанных данных, которые не позволяют установить конкретное устройство или пользователя, включая статистическую информацию, в следующих целях:</p> <ul style="list-style-type: none"> <li>• проведение исследований в области кибербезопасности;</li> <li>• расширение возможностей для выявления вредоносного ПО и киберугроз, в том числе за счет анализа выборочных данных;</li> <li>• отслеживание и публикация отчетов о тенденциях и рисках в области безопасности (включая кражу персональных данных);</li> <li>• проведение статистического анализа применительно к используемым продуктам, включая оценку тенденций и сравнение с данными в базе агрегированных данных пользователей; и</li> <li>• контроль и усовершенствование параметров работы продуктов с точки зрения их доступности и времени реагирования.</li> </ul>

## Norton Identity Safe

Описание Продукта или Сервиса	Условия доступа и сбора данных	Обработка информации
<p>Norton Identity Safe может использоваться двумя способами: а) в качестве одного из компонентов Norton Security; и б) в виде расширения любого известного веб-браузера, за исключением Internet Explorer. В обоих случаях поддерживается менеджер паролей, который управляет именами пользователей, паролями и другой информацией, используемой при работе в сети Интернет.</p>	<p>1. Сведения об абоненте, устройстве и ПО, включая: название, версию и предпочитаемый язык веб-браузера; тип и версию операционной системы; IP-адрес пользовательского устройства; * другие указываемые пользователем Персональные данные, которые могут в том числе включать имена пользователей, пароли, адреса веб-сайтов, физические адреса, сведения о платежных счетах и сроке действия и текстовую информацию в произвольном формате</p> <p>2. Данные об использовании сервиса, включая: сведения о посещаемых веб-сайтах; ключевые слова, используемые для поиска; информацию, заданную по умолчанию в различных окнах поиска, управляемых продуктами Norton; результаты поиска</p>	<p>1. Данные об устройстве и ПО обрабатываются Symantec в следующих целях:</p> <ul style="list-style-type: none"> <li>• обеспечение работоспособности и повышение эффективности работы Сервисов;</li> <li>• управление лицензиями;</li> <li>• оценка параметров использования продукта и предпочтений пользователей в целях индивидуализации оказываемых услуг и повышения эффективности работы с продуктом;</li> <li>• оказание пользователю содействия при установке программного обеспечения;</li> <li>• совершенствование Продуктов и Сервисов, повышение степени защиты пользователя, сети, устройства, данных и личности пользователя; и</li> <li>• повышение удовлетворенности пользователей качеством обслуживания за счет использования своих собственных или сторонних контакт-центров.</li> </ul> <p>2. Данные об использовании Продукта обрабатываются Symantec и уполномоченными ею лицами в следующих целях:</p> <ul style="list-style-type: none"> <li>• информирование пользователя о безопасности той или иной площадки;</li> <li>• блокировка доступа к небезопасным веб-сайтам; и</li> <li>• анализ использования Сервиса.</li> </ul> <p><a href="#">Обезличенные IP-адреса</a> и данные об использовании продуктов обрабатываются Протоколом передачи статистических данных (Measurement Protocol) <a href="#">Google Analytics</a> для статистического анализа и управления критическими ошибками. Для получения дополнительной информации см. <a href="#">информацию о средствах защиты данных Google Analytics</a>.</p> <p>Кроме того, Symantec использует полученную информацию для создания агрегированных, обезличенных и иным образом обработанных данных, которые не позволяют установить конкретное устройство или пользователя, включая статистическую информацию, в следующих целях:</p> <ul style="list-style-type: none"> <li>• проведение исследований в области кибербезопасности;</li> <li>• расширение возможностей для выявления вредоносного ПО и киберугроз, в том числе за счет анализа выборочных данных;</li> <li>• отслеживание и публикация отчетов о тенденциях и рисках в области безопасности (включая кражу персональных данных);</li> <li>• проведение статистического анализа применительно к используемым продуктам, включая оценку тенденций и сравнение с данными в базе агрегированных данных пользователей; и</li> <li>• контроль и усовершенствование параметров работы продуктов с точки зрения их доступности и времени реагирования.</li> </ul>



## Norton Family Premier

Описание Продукта или Сервиса	Условия доступа и сбора данных	Обработка информации
<p>Norton Family Premier защищает подключенных к сервису пользователей и указанные абонентом устройства путем использования средств родительского контроля, параметры которых задаются в настройках и функциях, задаваемых и управляемых абонентом.</p> <p>Для получения дополнительной информации о Norton Family Premier см. раздел «Дополнительная информация о Norton Family Premier» ниже.</p>	<p>*1. Сведения об абоненте, включая: контактные данные администратора (в том числе ФИО, адрес электронной почты и пароль доступа к учетной записи абонента); Персональные данные, указанные абонентом при настройке Сервиса или в ходе последующих телефонных переговоров со службой поддержки;</p> <p>2. Данные об устройстве и ПО, включая: сведения о ходе установки клиентского ПО Norton Family на устройство абонента или подключенного к сервису пользователя; настройки ПО, сведения о продуктах и информации о ходе установки; сведения о лицензии и лицензионных правах; идентификационный номер лицензии; информацию об использовании лицензии; название, тип, версию и язык операционной системы и местонахождение устройства (глобальная система определения местоположения); тип и версию веб-браузера; сведения об аппаратных средствах, ПО и установленных на устройстве приложениях; параметры доступа к приложениям и базе данных; сведения о действующих политиках и их соблюдении; журналы исключений приложений и журналы ошибок, обнаруженных при выполнении рабочих процессов;</p> <p>*3. Сведения о подключенных к сервису пользователях, передаваемые Symantec абонентом, включая: ФИО, пол, возраст и год рождения; графическое изображение (аватар); последние шесть цифр официального идентификационного номера подключенного к сервису пользователя (например, при наличии, номера социального страхования и национального идентификационного номера); адрес электронной почты; номер мобильного телефона; название университета и другие данные, выбранные для защиты абонентом; данные для входа в учетную запись машины; страну и часовой пояс;</p> <p>4. Данные о работе подключенного к сервису пользователя в сети, отслеживаемые Symantec по указанию абонента, в том числе (исключительно на усмотрение абонента): сведения о работе в сети Интернет и пользовании мобильным устройством; данные о местонахождении; открываемые подключенным к сервису пользователем веб-сайты, в</p>	<p>1. Информация об абоненте обрабатывается Symantec в следующих целях:</p> <ul style="list-style-type: none"> <li>• обеспечение работоспособности и повышение эффективности работы Norton Family;</li> <li>• оказание услуг поддержки и содействие при устранении ошибок и сбоев;</li> <li>• рассылка абонентам рекламных материалов (с разрешения абонента или иным образом в порядке, не противоречащем применимым законам); и</li> <li>• настройка учетной записи Norton абонента.</li> </ul> <p>2. Данные об устройстве и ПО обрабатываются Symantec в следующих целях:</p> <ul style="list-style-type: none"> <li>• обеспечение нормальной работы Продукта и предоставление абоненту доступа к указанным в заявке Сервисам;</li> <li>• управление лицензиями;</li> <li>• оценка и повышение коэффициента успешной установки Продукта;</li> <li>• проведение исследований и разработок в целях усовершенствования продуктов и сервисов Symantec и оптимальной защиты сети, устройств, информации и идентификационных данных абонента и подключенных к сервису пользователей.</li> </ul> <p>3. Сведения о подключенных к сервису пользователях обрабатываются в следующих целях:</p> <ul style="list-style-type: none"> <li>• идентификация и аутентификация Symantec абонента и подключенных к сервису пользователей;</li> <li>• оказание абоненту содействия в выявлении случаев несанкционированного использования Персональных данных подключенных к сервису пользователей; и</li> <li>• взаимодействие с абонентом и с его разрешения с подключенным к сервису пользователем для предоставления доступа к Сервису.</li> </ul> <p>4. Сведения о действиях подключенных к сервису пользователей обрабатываются в следующих целях:</p> <ul style="list-style-type: none"> <li>• оказание абоненту содействия в контроле за действиями, совершаемыми с использованием устройств подключенных к сервису пользователей в сети Интернет;</li> <li>• сведение к минимуму ущерба, который может быть нанесен установленным вредоносным ПО;</li> <li>• оказание абоненту содействия в обеспечении соблюдения установленных абонентом правил, регулирующих действия в сети Интернет, совершаемые с использованием устройств подключенных к сервису пользователей;</li> <li>• оказание абоненту содействия в обнаружении угроз, которым могут быть подвержены подключенные к сервису пользователи, с использованием средств</li> </ul>

	<p>том числе заблокированные Продуктом веб-сайты; ключевые слова, использованные подключенным к сервису пользователем при поиске информации в сети Интернет; устанавливаемые и удаляемые таким пользователем приложения (при условии что абонент активировал функцию контроля выполняемых с приложениями операций); время использования устройства подключенным к сервису пользователем; *название и адрес профиля, возраст, адрес страницы в Facebook и просмотренные пользователем видеоматериалы; видеоролики, просмотренные пользователем на YouTube.com и (или) Hulu (при условии что абонент активировал функцию контроля просматриваемых видеоматериалов).</p>	<p>интерактивного взаимодействия, службы мультимедийных и коротких текстовых сообщений; и</p> <ul style="list-style-type: none"> <li>оказание абоненту содействия в защите подключенных к сервису пользователей от вышеназванных угроз.</li> </ul> <p>Кроме того, Symantec использует полученную информацию для создания агрегированных, обезличенных и иным образом обработанных данных, которые не позволяют установить конкретное устройство или пользователя, включая статистическую информацию, в следующих целях:</p> <ul style="list-style-type: none"> <li>проведение исследований в области кибербезопасности;</li> <li>расширение возможностей для выявления вредоносного ПО и киберугроз, в том числе за счет анализа выборочных данных;</li> <li>отслеживание и публикация отчетов о тенденциях и рисках в области безопасности (включая кражу персональных данных); и</li> <li>проведение статистического анализа применительно к используемым продуктам, включая оценку тенденций и сравнение с данными в базе агрегированных данных пользователей.</li> </ul>
--	---	--

## Дополнительная информация о Norton Family Premier

При подключении абонента к данному сервису Norton Family исключает разглашение Персональных данных подключенными пользователями.

В случаях, не запрещенных применимым законодательством страны или территории, где находится абонент, Symantec может предоставлять доступ к сервису **Text Message Supervision**, который позволяет абоненту контролировать и блокировать текстовые (SMS) и мультимедийные (MMS) сообщения, отправляемые на мобильный телефон подключенного к сервису пользователя (или в обратном направлении), а также к сервису **Location Monitoring**. Возможности по контролю отправляемых и принимаемых текстовых и мультимедийных сообщений и (или) местоположения и использованию результатов такого контроля могут быть ограничены применимым законодательством страны места нахождения абонента (вплоть до полного запрета таких действий). Перед подключением к данному сервису следует обратиться за консультацией в местные уполномоченные органы.

После подключения абонента к сервису Location Monitoring служба Norton Family будет выполнять указания абонента и использовать глобальную систему определения местоположения для отслеживания и сбора данных о местонахождении указанного абонентом мобильного устройства. Для отслеживания, сбора, использования и разглашения данных о местонахождении указанного абонентом устройства Norton Family требуется разрешение абонента и (в зависимости от обстоятельств) пользователя мобильного устройства или его родителей. Такие разрешения оформляются через Интернет-портал Norton или (в зависимости от обстоятельств) могут быть неотъемлемой частью продукта и требовать подтверждения при вводе данных банковской карты при оплате абонентом Сервиса Symantec в сети Интернет. Вы можете в любое время отозвать такое согласие. Для получения дополнительной информации см. раздел «Ваши права в области конфиденциальности» в [Глобальном заявлении Symantec-Norton о конфиденциальности](#). После отключения от Сервиса данные учетной записи абонента, связанной с этим Сервисом, будут удалены.

При загрузке абонентом приложения на указанном мобильном устройстве Symantec может собирать данные о его местонахождении, даже если приложение не используется. Эти данные о местоположении передаются исключительно абоненту, который получает возможность контролировать местонахождение устройства; при этом Symantec обрабатывает эту информацию исключительно в производственных целях для оказания услуг и предоставления абоненту доступа к заказанным функциям. Абонент не вправе пользоваться сервисом контроля местонахождения, поддерживаемым продуктом, для отслеживания данных, местоположения, действий и другой информации, связанной с любым лицом, родителем которого абонент не является. Абоненты, расположенные в пределах Европейского экономического пространства, обязаны провести беседу с подключенными к сервису пользователями, родителями которых они являются (в особенности, если речь идет о пользователях в возрасте 13 лет и старше), и принять меры, гарантирующие, что вышеназванные пользователи понимают и осознают, что подразумевает использование Продукта и связанных с ним Сервисов. При принятии решения об использовании Продукта и связанных с ним Сервисов абонент несет исключительную ответственность за соблюдение законов и прочих нормативных актов, регулирующих взаимоотношения абонента с подключенными к сервису пользователями, родителем которых он является, и связанные с этим обязанности.

### Text Message Supervision

Сервис Text Message Supervision по умолчанию выключен. При необходимости абонент должен включить Text Message Supervision и установить Norton Family на подконтрольное

мобильное устройство. После активации сервиса Text Message Supervision получает от контролируемого устройства следующие сведения:

- номер мобильного телефона, присвоенного контролируемому мобильному устройству, и номера мобильных телефонов других устройств, с которыми осуществляется обмен текстовыми и мультимедийными сообщениями;
- содержание отправленных и полученных контролируемым устройством текстовых сообщений (применительно к мультимедийным сообщениям Symantec не сохраняет и не получает сведения о содержании таких сообщений; в этом случае регистрируется сам факт обмена мультимедийными сообщениями);
- имя адресной книги (при наличии), с которой на контролируемом устройстве связан номер мобильного телефона, используемый для отправки текстовых и мультимедийных сообщений на контролируемое устройство (и в обратном направлении);
- дата и время обмена сообщениями;
- местонахождение контролируемого устройства;
- журнал событий с заблокированными текстовыми и мультимедийными сообщениями (с указанием номеров телефонов сторон и имен, если они указаны в адресной книге на контролируемом устройстве).

Перед тем как начинать контролировать текстовые и мультимедийные сообщения, отправляемые и (или) принимаемые на указанном абонентом мобильном устройстве, Symantec отправляет на такое устройство предупредительное текстовое сообщение, уведомляя пользователя такого устройства о выполнении указаний абонента, записи и контроле содержания вышеназванных текстовых и мультимедийных сообщений. Если после получения такого предупредительного текстового сообщения с указанного абонентом устройства продолжается отправка (или прием) текстовых и мультимедийных сообщений, Symantec начинает регистрировать и контролировать такие сообщения в целях, указанных в настоящем Уведомлении, в соответствии с указаниями абонента. Symantec отправляет такое предупредительное текстовое сообщение на контролируемое устройство повторно на ежемесячной основе или перед очередным сеансом связи.

В случае если абонент принимает решение заблокировать все текстовые и мультимедийные сообщения, которыми пользователь контролируемого устройства обменивается с тем или иным пользователем, Symantec уведомляет об этом пользователя контролируемого устройства и отправляет текстовое сообщение другой стороне, уведомляя о блокировке таких сообщений и невозможности осуществить их доставку.