
Acronis Ransomware Protection

Содержание

1 Введение

1.1 Что такое Acronis Ransomware Protection

Acronis Ransomware Protection — это пакет программ, гарантирующий безопасность информации на ПК. Он объединяет две дополняющие друг друга функции, которые обеспечивают дополнительную защиту личных данных:

- **Acronis Active Protection**

  Эта служба защищает компьютер от программ-вымогателей — вредоносных программ, которые блокируют доступ к некоторым файлам или всей системе и требуют заплатить за разблокировку. Служба Acronis Active Protection, основанная на эвристическом методе, отслеживает процессы, запущенные на компьютере, в режиме реального времени. Обнаружив сторонний процесс, который пытается зашифровать файлы или внедрить вредоносный код в нормальный процесс, Acronis Ransomware Protection уведомляет пользователя и предлагает разрешить процессу изменять файлы или заблокировать процесс. Даже если файлы были зашифрованы программой-вымогателем, их можно восстановить из временных копий. Дополнительные сведения см. в разделе Acronis Active Protection (стр. 11).

- **Резервное копирование на уровне файлов в Acronis Cloud**

  Вы можете защитить документы, фотографии, музыкальные файлы и видеозаписи от повреждения или потери путем резервного копирования в защищенное хранилище Acronis Cloud. Поскольку файлы находятся в удаленном хранилище, они будут защищены даже в случае потери, кражи или поломки компьютера. При необходимости все данные можно восстановить на новое устройство. Изменения в защищенных файлах автоматически загружаются в облачное хранилище для поддержания актуальности резервной копии. Вместе с Acronis Ransomware Protection вы бесплатно получаете 5 ГБ в облачном хранилище. Если этого недостаточно, можно купить дополнительное пространство. Дополнительные сведения см. в разделе Резервное копирование файлов и папок (стр. 8).

Acronis Mobile

Пространство в хранилище Acronis Cloud можно использовать для защиты данных не только на компьютере, но и на мобильных устройствах. Acronis Mobile — это бесплатное приложение, которое позволяет выполнять резервное копирование данных в Acronis Cloud, а затем восстанавливать их в случае потери или повреждения на то же или новое мобильное устройство. Приложение поддерживает смартфоны и планшеты под управлением операционных систем iOS и Android. Дополнительные сведения см. в разделе Acronis Mobile (стр. 15).

С помощью приложения Acronis True Image для настольных ПК или Acronis True Image для NAS можно выполнить резервное копирование данных мобильного устройства на компьютер или устройство NAS. Дополнительные сведения см. в разделе Обновление Acronis Ransomware Protection (стр. 4).

1.2 Системные требования

Для работы Acronis Ransomware Protection необходимо следующее оборудование.

- Процессор Pentium с тактовой частотой 1 ГГц.

- 1 ГБ ОЗУ.
- 1,5 ГБ свободного пространства на жестком диске.
- Разрешение экрана 1024 x 768.
- Мышь или другое указывающее устройство (рекомендуется).

Другие требования:

- Подключение к Интернету
- Права администратора для запуска Acronis Ransomware Protection

Операционные системы

- Windows 7 SP1 (все выпуски)
- Windows 8 (все выпуски)
- Windows 8.1 (все выпуски)
- Windows 10 (все выпуски)

1.3 Установка Acronis Ransomware Protection

Установка Acronis Ransomware Protection

Как установить Acronis Ransomware Protection

1. Запустите файл установки. Прежде чем начать процесс установки, Acronis Ransomware Protection проверяет наличие более новой версии на веб-сайте. Если новая версия доступна, она будет предложена для установки.
2. Нажмите кнопку **Установить**.

   Acronis Ransomware Protection будет установлен на системный раздел (обычно C:).
3. В открывшемся окне выполните вход в свою учетную запись Acronis.

   Дополнительные сведения см. в разделе Учетная запись Acronis (стр. 6).

Удаление Acronis Ransomware Protection

Выберите **Пуск** -> **Настройки** -> **Панель управления** -> **Установка и удаление программ** -> **Acronis Ransomware Protection** -> **Удалить**. Затем следуйте инструкциям на экране. После этого необходимо перезагрузить компьютер для завершения задания.

Если используется ОС Windows 10, щелкните **Пуск** -> **Параметры** -> **Система** -> **Приложения и возможности** -> **Acronis Ransomware Protection** -> **Удалить**.

Если используется ОС Windows 8, щелкните значок «Параметры» и выберите **Панель управления** -> **Удаление программы** -> **Acronis Ransomware Protection** -> **Удалить**.

Если используется ОС Windows 7, щелкните **Пуск** -> **Панель управления** -> **Удаление программы** -> **Acronis Ransomware Protection** -> **Удалить**.

1.4 Обновление Acronis Ransomware Protection

Acronis Ransomware Protection позволяет выполнять резервное копирование только файлов и папок и только в Acronis Cloud. Если необходимо резервное копирование всех данных на компьютере или отдельных разделов, следует обновить продукт до Acronis True Image. Этот продукт предоставляет полный набор функций для защиты данных, включая резервное копирование на уровне файлов и дисков в локальное хранилище, на устройство NAS или в

Acronis Cloud, архивирование данных, синхронизацию данных, защиту данных на мобильных устройствах и многое другое.

Чтобы выполнить обновление, просто установите Acronis True Image на компьютере с установленным продуктом Acronis Ransomware Protection. Acronis True Image можно приобрести на веб-сайте Acronis.

Как купить дополнительное пространство в Acronis Cloud

1. Запустите Acronis Ransomware Protection.
2. Щелкните значок учетной записи и выберите **Купить дополнительное пространство**. Откроется веб-сайт Acronis.
3. Выберите нужную квоту хранилища и введите свои платежные данные.

1.5 Техническая поддержка

Поддержка Acronis Ransomware Protection основана на ресурсах сообщества и представлена в виде базы знаний Acronis и форума Acronis Ransomware Protection.

2 Приступая к работе

В этом разделе

2.1 Учетная запись Acronis

Для работы Acronis Ransomware Protection необходимо выполнить вход в свою учетную запись Acronis. При выходе из учетной записи Acronis Active Protection продолжает работать, но приложение перестает обновлять резервную копию в облаке.

Как создать учетную запись Acronis

После первого запуска Acronis Ransomware Protection отображается форма регистрации.

Если у вас еще нет учетной записи Acronis

1. Заполните форму регистрации.

   Для безопасности своих личных данных выберите надежный пароль, следите за тем, чтобы этот пароль не попал в руки злоумышленников, и время от времени меняйте его.

2. Щелкните **Создать учетную запись**.
3. На указанный адрес электронной почты будет отправлено сообщение. Откройте его и подтвердите создание учетной записи.

Как выполнить вход

Как выполнить вход в учетную запись Acronis

1. Чтобы переключиться с формы регистрации на форму входа, щелкните **У меня уже есть учетная запись**.
2. Введите адрес электронной почты и пароль, которые использовались при регистрации, после чего нажмите **Вход**.

Как выполнить выход

Как выполнить выход из учетной записи Acronis

1. Запустите Acronis Ransomware Protection.
2. Щелкните значок учетной записи и выберите **Выход**.

2.2 Начало работы с Acronis Cloud

Услуга Acronis Cloud может быть недоступна для вашего региона. Щелкните здесь, чтобы получить дополнительные сведения https://kb.acronis.com/content/4541 https://kb.acronis.com/content/4541

Удаленное хранилище

С одной стороны, Acronis Cloud — это защищенное удаленное хранилище, которое можно использовать для хранения резервных копий файлов и папок. Вместе с Acronis Ransomware Protection вы бесплатно получаете 5 ГБ в облачном хранилище. Если этого недостаточно для защиты ваших файлов, можно купить дополнительное пространство. Дополнительные сведения см. в разделе Обновление Acronis Ransomware Protection (стр. 4).

Поскольку файлы находятся в удаленном хранилище, они будут защищены даже в случае кражи компьютера или пожара в доме. В случае аварии или повреждения данных вы всегда сможете восстановить файлы.

С помощью одной учетной записи можно сохранить данные с нескольких компьютеров и всех ваших мобильных устройств с операционными системами iOS и Android.

Веб-приложение

С другой стороны, Acronis Cloud — это веб-приложение, позволяющее восстановить данные, которые хранятся в Acronis Cloud, и управлять этими данными. Для работы с приложением можно использовать любой компьютер, подключенный к Интернету.

Для доступа к приложению перейдите по адресу https://www.acronis.com/ru-ru/my/online-backup/webrestore/ и войдите в свою учетную запись Acronis.

2.2.1 Как мы обеспечиваем защиту ваших данных

Когда вы используете Acronis Cloud в качестве хранилища резервных копий, архивов и синхронизированных данных, вам необходима гарантия того, что ваши личные файлы не попадут в руки злоумышленников. Возможно, вас особенно беспокоит безопасность использования мобильного устройства, поскольку все данные будут передаваться через Интернет.

Компания Acronis гарантирует сохранность ваших данных. Прежде всего мы используем протоколы с шифрованием (SSL, TLS) для передачи всех данных как через Интернет, так и по локальной сети. Для доступа к данным выполните вход в свою учетную запись, указав адрес электронной почты и пароль.

Более того, данные хранятся на наших серверах в зашифрованной форме. Только у вас есть доступ к зашифрованным данным.

3 Резервное копирование данных

В этом разделе

3.1 Резервное копирование файлов и папок

Acronis Ransomware Protection позволяет выполнять резервное копирование документов, фотографий, музыкальных файлов и видеозаписей в Acronis Cloud. В случае потери или повреждения этих файлов на компьютере их легко можно восстановить из облачного хранилища.

Резервное копирование файлов и папок

1. Запустите Acronis Ransomware Protection.
2. Откройте шаг настройки резервного копирования в руководстве или главное окно приложения.
3. Чтобы указать файлы и папки для резервного копирования, выполните одно из следующих действий.
   - В проводнике или другом диспетчере файлов выделите нужные файлы и папки, а затем перетащите их в окно Acronis Ransomware Protection.
   - Щелкните **Добавить их вручную**, а затем перейдите к нужным папкам на дисках.

   Резервное копирование запустится автоматически.

Первое резервное копирование может занять значительное время. Последующие операции резервного копирования должны происходить намного быстрее, так как через Интернет будут передаваться только изменения в файлах. Acronis Ransomware Protection проверяет изменения в данных каждые 15 минут и автоматически загружает их в Acronis Cloud.

Чтобы изменить параметры резервного копирования, щелкните значок шестерни в главном окне приложения.

Правила хранения

Поскольку Acronis Ransomware Protection постоянно отслеживает данные резервного копирования и загружает изменения в Acronis Cloud, резервные копии могут довольно быстро заполнить место в хранилище. Чтобы сократить количество версий файлов и оптимизировать потребление пространства в облаке, Acronis Ransomware Protection хранит только следующие версии файлов:

- Все версии за последний час
- Первые версии каждого часа за последние 24 часа
- Первую версию каждого дня за последнюю неделю
- Первую версию каждой недели за последний месяц
- Первую версию каждого месяца

Все остальные версии автоматически удаляются. Правила хранения предустановлены и не меняются.

3.2 Удаление данных из Acronis Cloud

Поскольку свободное пространство в Acronis Cloud ограниченно, необходимо следить за ним, удаляя устаревшие или ненужные данные. Онлайн-хранилище может быть очищено несколькими способами.

Удаление целой резервной копии

Наиболее радикальный способ — удаление всей резервной копии из Acronis Cloud.

Как удалить резервную копию целиком

1. Перейдите по адресу https://www.acronis.com/ru-ru/my/online-backup/webrestore/ и выполните вход в учетную запись Acronis.
2. На вкладке **Состояние хранилища** наведите курсор на резервную копию для удаления, щелкните значок шестерни и выберите **Удалить**.

Удаление отдельных файлов и папок

Также вы можете удалить из Acronis Cloud отдельные файлы и папки.

1. Перейдите по адресу https://www.acronis.com/ru-ru/my/online-backup/webrestore/ и выполните вход в учетную запись Acronis.
2. Выберите нужные файлы и папки и щелкните **Удалить**.

4 Восстановление данных

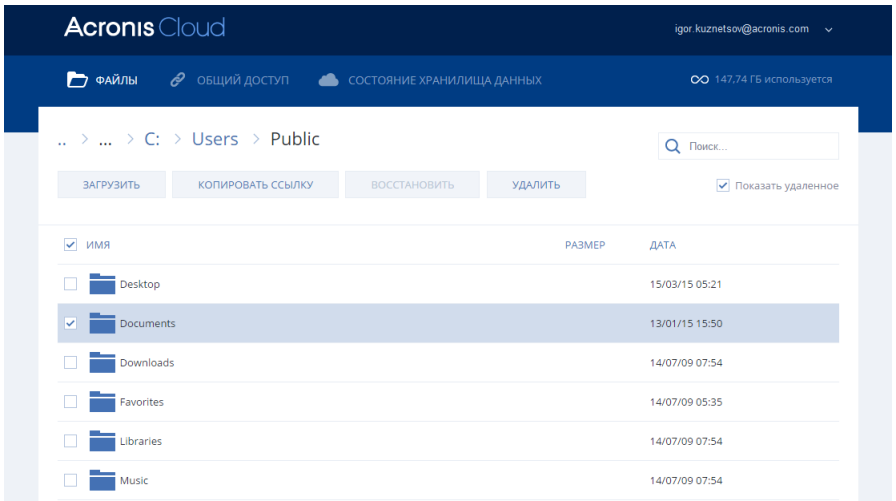
В этом разделе

4.1 Восстановление данных из Acronis Cloud

После сохранения резервных копий файлов в Acronis Cloud можно использовать веб-приложение Acronis Cloud для восстановления этих файлов на компьютер.

Как восстановить файлы и папки из Acronis Cloud

1. Чтобы открыть веб-приложение Acronis Cloud, выполните одно из нижеприведенных действий.
   - Перейдите по адресу https://www.acronis.com/ru-ru/my/online-backup/webrestore/ и выполните вход в свою учетную запись.
   - В главном окне Acronis Ransomware Protection щелкните значок учетной записи, выберите **Просмотр данных,** выполните вход в свою учетную запись и щелкните **Резервные копии**.
2. После загрузки вкладки **Files (Файлы)** на веб-сайте Acronis Cloud выберите нужную резервную копию в области **Backups (Резервные копии)**.
3. Выберите файлы и папки для восстановления. Нажмите кнопку **Download** (Загрузить), чтобы начать восстановление.



Если выбрано несколько файлов и папок, они будут помещены в ZIP-архив.

По умолчанию данные сохраняются в папку **Загрузки**. Путь загрузки можно изменить.

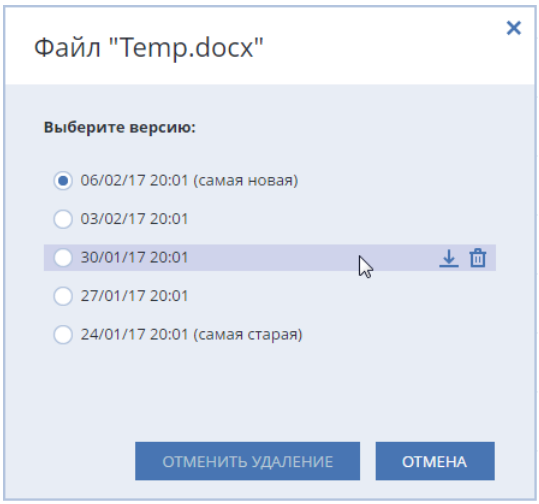
4.2 Восстановление версии файла

По умолчанию Acronis Ransomware Protection выбирает последние версии относительно указанной даты. При необходимости для восстановления можно выбрать определенную версию файла.

Учтите, что этот параметр неприменим к папкам.

Как выбрать отдельную версию файла

1. В списке содержимого резервной копии выберите файл, версию которого необходимо восстановить, и щелкните значок шестерни справа. Выберите **Просмотреть версии** в открывшемся меню.
2. В открывшемся окне наведите курсор на нужную версию и щелкните значок **Загрузить**.



По умолчанию данные сохраняются в папку **Загрузки**.

Дополнительные сведения о правилах хранения резервных копий см. в разделе Резервное копирование файлов и папок (стр. 8).

5 Acronis Active Protection

Что такое программа-вымогатель?

Это вредоносная программа, которая блокирует доступ к вашим файлам или всей системе и требует заплатить за разблокировку. Программа отображает окно с сообщением, что ваши файлы заблокированы и необходимо срочно заплатить, иначе вы потеряете к ним доступ. Сообщение также может быть замаскировано под заявление властей или полиции. Цель этого сообщения — запугать пользователя и заставить заплатить, не обращаясь за помощью к ИТ-специалисту или в полицию. Более того, даже если вы заплатите, восстановление доступа к данным не гарантировано.

Компьютер может быть атакован программой-вымогателем, когда пользователь заходит на небезопасный веб-сайт, открывает почтовые сообщения с неизвестных адресов или переходит по подозрительным ссылкам в соцсетях или мессенджерах.

Программа-вымогатель может заблокировать:

- **Весь компьютер**

  Вы не можете использовать Windows и выполнять какие-либо действия на компьютере. Как правило, в этом случае программа-вымогатель не шифрует ваши данные.
- **Отдельные файлы**

Обычно это личные данные, такие как документы, фотографии и видео. Программа-вымогатель шифрует файлы и требует заплатить за ключ, без которого расшифровать данные нельзя.

- **Приложения**

  Программа-вымогатель блокирует некоторые приложения, не позволяя их запускать. Чаще всего атакуется веб-браузер.

Как Acronis Ransomware Protection защищает ваши данные от программ-вымогателей

Для защиты компьютера от программ-вымогателей Acronis Ransomware Protection использует технологию Acronis Active Protection. Эта технология, основанная на эвристическом методе, отслеживает процессы, запущенные на компьютере, в режиме реального времени. Обнаружив сторонний процесс, который пытается зашифровать файлы или внедрить вредоносный код в нормальный процесс, Acronis Ransomware Protection уведомляет пользователя и предлагает разрешить процессу изменять файлы или заблокировать процесс. Дополнительные сведения см. в разделе Защита данных от программ-вымогателей (стр. 13).

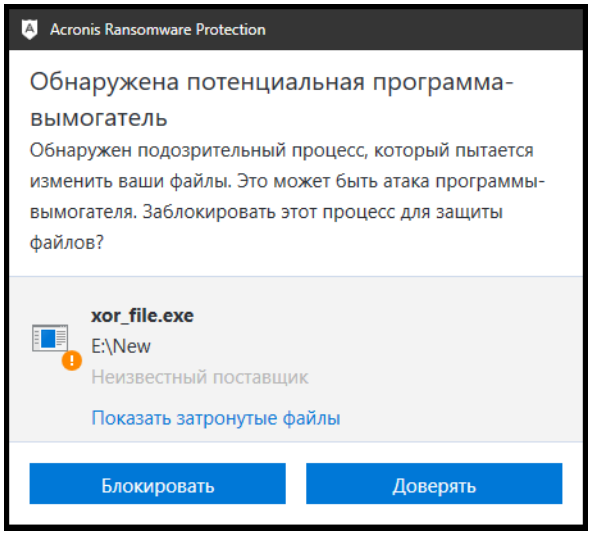
Эвристический подход широко используется в современном антивирусном ПО как эффективный способ защиты от вредоносных программ. В отличие от анализа сигнатур, который позволяет обнаружить только один образец, эвристический анализ определяет семейства вредоносных программ, включающие образцы с похожим поведением. Еще одно преимущество этого подхода — возможность обнаруживать новые виды вредоносных программ, для которых еще нет сигнатур.

Acronis Active Protection использует эвристический метод для анализа цепочки действий, выполненных программой, которые затем сравниваются с цепочкой событий в базе данных, содержащей модели поведения вредоносных программ. Поскольку это неточный метод, существует возможность ложного срабатывания, когда доверенная программа определяется как вредоносная. Чтобы исключить подобные ситуации, Acronis Active Protection выдает запрос о доверии обнаруженному процессу. Если этот же процесс будет обнаружен второй раз, его можно добавить в список разрешений и задать для него действие по умолчанию, пометив как доверенный или заблокированный. Либо можно добавить процесс в черный список. В этом случае процесс будет блокироваться при каждой попытке изменить файлы.

Чтобы собрать как можно больше различных моделей поведения, Acronis Active Protection использует машинное обучение. Эта технология основана на математической обработке больших данных, полученных с помощью телеметрии. Это самообучающаяся система, поскольку чем больше данных обрабатывается, тем точнее определяется принадлежность процесса к программам-вымогателям.

5.1 Защита данных от программ-вымогателей

Когда служба Acronis Active Protection включена, она отслеживает процессы, запущенные на компьютере, в режиме реального времени. Обнаружив сторонний процесс, который пытается зашифровать файлы, служба уведомляет пользователя и предлагает разрешить процессу изменять файлы или заблокировать процесс.



Перед принятием решения можно просмотреть список файлов, которые процесс собирается изменить.

Чтобы разрешить процессу изменять файлы, щелкните **Доверять**. Если вы не уверены в безопасности и правомерности процесса, рекомендуем выбрать **Блокировать**. В любом случае при следующем запуске этого процесса Acronis Ransomware Protection снова выдаст запрос. Чтобы дать процессу постоянное разрешение или блокировать его при каждой попытке изменить файлы, установите флажок **Запомнить выбор для этого процесса**, а затем щелкните **Блокировать** или **Доверять**. Процесс будет добавлен в список разрешений. Управление списком доступно в разделе «Настройки».

После блокировки процесса рекомендуется проверить, не были ли файлы зашифрованы или повреждены. Если это произошло, щелкните **Восстановить измененные файлы**. Acronis Ransomware Protection выполнит поиск последних версий файлов и восстановит файлы из временных копий, которые были созданы ранее во время проверки процесса.

Чтобы это действие выполнялось по умолчанию, установите флажок **Всегда восстанавливать файлы после блокировки процесса**.

5.2 Управление Acronis Active Protection

Когда служба Acronis Active Protection включена, она отслеживает процессы, запущенные на компьютере, в режиме реального времени. Обнаружив сторонний процесс, который пытается зашифровать файлы, служба уведомляет пользователя и предлагает разрешить процессу изменять файлы или заблокировать процесс. Дополнительные сведения см. в разделе Acronis Active Protection (стр. 11).

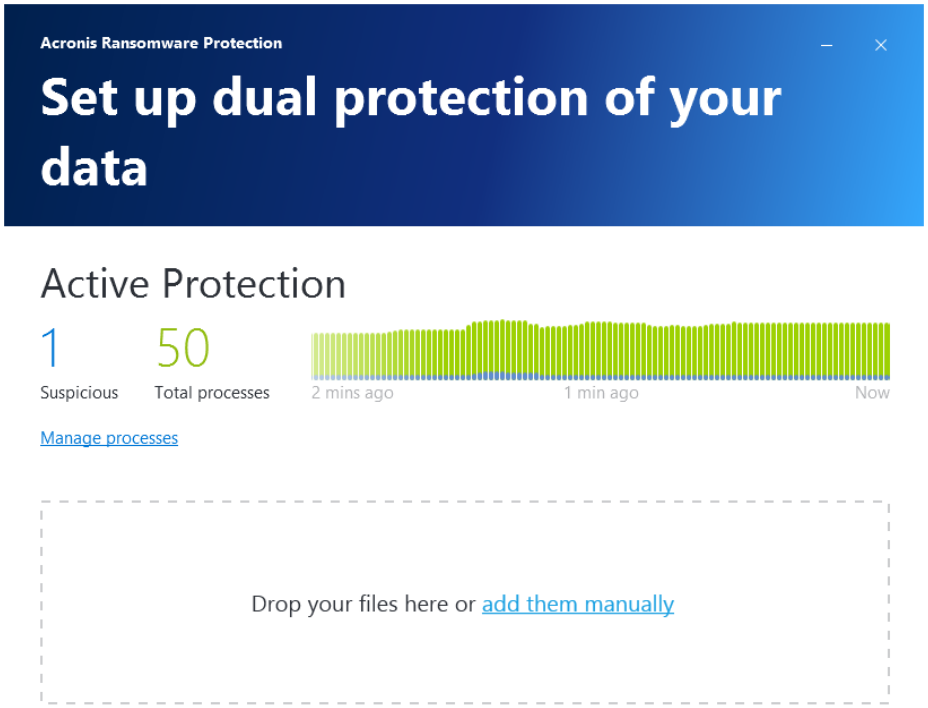
Настроить параметры Acronis Active Protection и контролировать процесс защиты можно в следующих местах:

- Раздел Acronis Active Protection

- Область уведомлений на панели задач Windows

Раздел Acronis Active Protection

В этом разделе можно просмотреть статистику процесса защиты и настроить список разрешений Acronis Active Protection.



Можно выполнить следующие действия.

- Просмотреть в режиме реального времени количество отслеживаемых и безопасных процессов.
- Управлять списком разрешений, чтобы отметить как доверенные или блокировать приложения.

Область уведомлений на панели задач Windows

Щелкнув правой кнопкой мыши значок в области уведомлений, можно открыть следующие элементы меню:

- **Отключить Active Protection** (**включить Active Protection**) — отключение и включение защиты от программ-вымогателей.
- **Открыть** — открытие главного окна приложения.

6 Acronis Mobile

Услуга Acronis Cloud может быть недоступна для вашего региона. Щелкните здесь, чтобы получить дополнительные сведения https://kb.acronis.com/content/4541 https://kb.acronis.com/content/4541

Acronis Mobile позволяет выполнять резервное копирование данных в Acronis Cloud, а затем восстанавливать их в случае потери или повреждения.

Какие устройства поддерживают мобильное приложение?

Acronis Mobile можно установить на любое мобильное устройство под управлением одной из следующих операционных систем:

- iOS 8.0 и выше (iPhone, iPad, iPod)
- Android 4.1 и выше (смартфоны и планшеты)

Основные функции

Acronis Mobile позволяет:

- выполнять резервное копирование личных данных, включая:
  - Фотографии
  - Видеозаписи
  - Фотографии и видеозаписи в iCloud (только на устройствах iOS)
  - Контакты
  - Календари
  - Сообщения (только на устройствах Android)
  - Напоминания (только на устройствах iOS)
- шифровать резервные копии с помощью алгоритма шифрования AES-256;
- выполнять автоматическое резервное копирование новых и измененных данных;
- получать доступ к облачным резервным копиям со всех ваших мобильных устройств и восстанавливать данные из этих резервных копий.

Где найти эти приложения?

Вы можете просмотреть дополнительные сведения и загрузить Acronis Mobile в Apple App Store или Google Play.

- Acronis Mobile для устройств iOS:
  https://itunes.apple.com/us/app/acronis-true-image-cloud/id978342143
- Acronis Mobile для устройств Android:
  https://play.google.com/store/apps/details?id=com.acronis.acronistrueimage

В этом разделе

6.1 Установка Acronis Mobile

В зависимости от используемого мобильного устройства зайдите в Apple App Store или Google Play и выполните поиск приложения Acronis Mobile.

Например, чтобы найти и установить Acronis Mobile для iOS, выполните следующее.

1. На телефоне iPhone откройте **App Store**.
2. Нажмите значок поиска.
3. Введите **acronis** в строку поиска.
4. Выберите **acronis mobile** в результатах поиска, чтобы перейти на страницу приложения.
5. Следуйте стандартной процедуре установки.

Поиск и установка приложения для Android выполняется похожим образом.

6.2 Резервное копирование мобильного устройства в Acronis Cloud

Мобильная резервная копия — это ваша гарантия сохранности данных на мобильном устройстве, которые можно будет восстановить в случае повреждения или потери. Также с помощью резервной копии можно перенести личные данные и настройки со старого смартфона на новый. Дополнительные сведения см. в разделе Acronis Mobile (стр. 15).

Создание резервной копии мобильных данных в Acronis Cloud

1. Запустите Acronis Mobile.
2. Выберите Acronis Cloud в качестве места назначения резервной копии.
3. Войдите в свою учетную запись Acronis.
4. Нажмите значок шестерни и выберите нужные категории данных либо нажмите **Создать резервную копию** для резервного копирования всех данных.
5. [необязательно] Нажмите **Использовать шифрование**, чтобы зашифровать и защитить резервную копию паролем. Либо нажмите **Пропустить**.
6. Нажмите **Создать резервную копию**.
7. Разрешите Acronis Mobile доступ к вашим личным данным.

После завершения резервного копирования ваши данные будут отправлены в защищенное хранилище Acronis Cloud. Если требуется автоматически выполнять резервное копирование изменений данных (например, новых фотографий), не забудьте включить параметр **Непрерывное резервное копирование**. Если этот параметр отключен, новые данные будут копироваться только при нажатии кнопки **Создать резервную копию**. Дополнительные сведения см. в разделе Параметры мобильного приложения (стр. 17).

6.3 Восстановление мобильных данных

Восстановление с помощью мобильного устройства

С помощью смартфона или планшета можно получить доступ к любой резервной копии мобильного устройства в Acronis Cloud. Как правило, можно открывать, просматривать, выполнять восстановление и некоторые другие операции с файлами или категорией данных. Обратите внимание, что из-за ограничений операционной системы некоторые операции могут быть недоступны для определенных типов файлов.

Доступ к мобильным данным с мобильного устройства

1. Установите и запустите Acronis Mobile.
2. Для доступа к резервной копии в облаке войдите в свою учетную запись Acronis, если потребуется.
3. Чтобы открыть боковое меню, проведите по экрану от левого края до правого, затем нажмите **Доступ и восстановление**.
4. Выберите резервную копию, которая содержит нужный файл или категорию данных. Резервную копию можно выбрать по имени или устройству, содержащему нужные данные. Например, для доступа к данным с вашего текущего мобильного устройства выберите это устройство из списка.
5. Перейдите к нужному файлу или категории данных.
6. В зависимости от типа данных можно выполнить следующие операции:
   - **Открыть**
   - **Восстановить**
   - **Восстановить все**

6.4 Восстановление данных на новый смартфон

При наличии мобильной резервной копии смартфона можно легко перенести личные данные на другое мобильное устройство. Например, это может быть удобно при покупке нового смартфона. Просто восстановите данные из Acronis Cloud на новое устройство.

Как восстановить данные на новый смартфон

1. Установите и запустите Acronis Mobile.
2. Нажмите **Резервное копирование в облако** и выполните вход в свою учетную запись Acronis.

   Acronis Mobile обнаружит резервные копии мобильного устройства в Acronis Cloud.
3. Нажмите **Восстановить данные**.
4. Выберите мобильное устройство, с которого следует восстановить данные, затем нажмите **Выбрать устройство**. Например, если требуется перенести данные со старого смартфона, выберите его.
5. Выберите категории данных, которые нужно восстановить, и нажмите кнопку **Восстановить**.
6. Разрешите Acronis Mobile доступ к вашим личным данным.

После завершения восстановления ваши данные будут загружены на новое устройство.

6.5 Параметры мобильного приложения

Чтобы открыть раздел **Параметры**, проведите по экрану от левого края до правого, затем нажмите кнопку **Параметры**. Параметры, доступные для выбора:

- **Непрерывное резервное копирование**

  Если этот параметр включен, Acronis Mobile автоматически обнаруживает новые данные и загружает их в Acronis Cloud.
- **Выполнять резервное копирование только с помощью Wi-Fi** или **Выполнять резервное копирование с помощью Wi-Fi и сотового подключения**

Можно выбрать тип подключения к Интернету, требуемый для отправки и загрузки данных. Это полезно, так как иногда подключение Wi-Fi дешевле (или бесплатно) либо более надежно, чем другие типы подключений.

- **Справка**

  Нажмите этот элемент, чтобы открыть веб-справку по продукту.

- **Отправить отзыв**

  Эта команда позволяет отправить отзыв о приложении Acronis Mobile, сообщить о проблеме или связаться со службой технической поддержки.

- **Очистить сохраненные пароли**

  Если при шифровании резервной копии выбрать параметр сохранения пароля, то приложение не будет запрашивать пароль при работе с данными резервной копии на мобильном устройстве. Выберите очистку сохраненных паролей, чтобы приложение запрашивало пароль при каждом доступе к резервной копии.

Заявление об авторских правах

С ПО или Услугой может быть предоставлен исходный код сторонних производителей. Лицензии этих сторонних производителей подробно описаны в файле license.txt, находящемся в корневом каталоге установки. Обновляемый список кода сторонних производителей и условия лицензии, применимые к программному обеспечению и/или службе, см. по адресу https://kb.acronis.com/content/7696

Запатентованные технологии Acronis

Технологии, которые использованы в этом продукте, регламентированы и защищены одним или несколькими нижеуказанными патентами США: 7,047,380; 7,246,211; 7,275,139; 7,281,104; 7,318,135; 7,353,355; 7,366,859; 7,383,327; 7,475,282; 7,603,533; 7,636,824; 7,650,473; 7,721,138; 7,779,221; 7,831,789; 7,836,053; 7,886,120; 7,895,403; 7,934,064; 7,937,612; 7,941,510; 7,949,635; 7,953,948; 7,979,690; 8,005,797; 8,051,044; 8,069,320; 8,073,815; 8,074,035; 8,074,276; 8,145,607; 8,180,984; 8,225,133; 8,261,035; 8,296,264; 8,312,259; 8,347,137; 8,484,427; 8,645,748; 8,732,121; 8,850,060; 8,856,927; 8,996,830; 9,213,697; 9,400,886; 9,424,678; 9,436,558; 9,471,441; 9,501,234; а также патентами, ожидающими выдачи.

7 Словарь терминов

А

Acronis Active Protection

Технология защиты данных от программ-вымогателей — вредоносных программ, которые блокируют доступ к вашим файлам или всей системе и требуют заплатить за разблокировку. Эта технология, основанная на эвристическом методе, отслеживает процессы, запущенные на компьютере, в режиме реального времени и сообщает пользователю о попытках зашифровать данные. Если файлы все-таки оказались зашифрованы, их можно восстановить из временных или резервных копий.

В

Версия резервной копии

Результат однократной операции резервного копирования (стр. 20). Физически это файл или набор файлов, содержащих резервные копии данных по состоянию на определенные дату и время. Файлы версий резервной копии, созданные программой Acronis Ransomware Protection, имеют расширение TIB. TIB-файлы, создаваемые в результате консолидации версий резервной копии, также называются версиями резервной копии.

Восстановление

Восстановление — это процесс возвращения поврежденных данных в нормальное состояние из резервной копии (стр. 21).

И

Инкрементная версия резервной копии

Версия резервной копии, в которой хранятся изменения, внесенные в данные после создания последней версии резервной копии. Для восстановления данных инкрементной версии резервной копии необходим доступ к другим версиям той же резервной копии.

Инкрементное резервное копирование

1. Метод резервного копирования, при котором сохраняются изменения, внесенные в данные после создания последней версии резервной копии (любого типа).
2. Процесс резервного копирования, при котором создается инкрементная версия резервной копии.

О

Операция резервного копирования

Эта операция создает копию данных жесткого диска машины для восстановления данных или возврата к состоянию на определенные дату и время.

П

Подозрительный процесс

Acronis Active Protection (стр. 20) использует эвристический метод для анализа цепочки действий, выполненных программой (процессом), которые затем сравниваются с цепочкой событий в базе данных, содержащей модели поведения вредоносных программ. Если программа пытается изменить файлы пользователя и ее поведение похоже на поведение программы-вымогателя, то она рассматривается как подозрительная.

Р

Резервная копия в онлайн-хранилище

Резервная копия в онлайн-хранилище — это резервная копия, созданная с помощью службы Acronis Online Backup. Такие

резервные копии хранятся в специальном хранилище, которое называется Acronis Cloud и доступно через Интернет. Таким образом, все резервные копии хранятся удаленно, что обеспечивает сохранность резервных копий независимо от локальных хранилищ пользователя. Для использования Acronis Cloud необходимо подписаться на услугу.

Резервное копирование

1. То же самое, что и операция резервного копирования (стр. 20).
2. Набор версий резервной копии, создаваемый и управляемый с помощью параметров резервного копирования. Резервная копия может содержать несколько версий данных, созданных с помощью полного и инкрементного (стр. 20) методов резервного копирования. Версии данных, принадлежащие к одной и той же резервной копии, обычно помещаются в одно хранилище.