**Что такое боты – определение и описание**



**Боты. Определение и описание**

«Бот» (сокращение от «робот») – это программа, выполняющая автоматические заранее настроенные повторяющиеся задачи. Боты обычно имитируют поведение пользователя или заменяют его. Боты являются автоматизированными, потому они работают намного быстрее, чем пользователи. Они выполняют полезные функции, например, обслуживание клиентов или индексация поисковых систем. Однако боты также могут являться вредоносными программами, используемыми для получения полного контроля над компьютером.

Интернет-боты также могут называться пауками, поисковыми роботами или веб-ботами.

**Что такое компьютерные и интернет-боты?**

Компьютерные и интернет-боты по сути являются цифровыми инструментами и, как любой инструмент, могут использоваться как во благо, так и во вред.

«Хорошие» боты выполняют полезные задачи, а «плохие» или вредоносные боты могут использоваться для взлома, рассылки спама, шпионажа, прерывания и взлома веб-сайтов любого размера. По [оценкам, в настоящее время до половины всего интернет-трафика](https://www.sciencedirect.com/science/article/pii/S0950705120302318) приходится на компьютерных ботов, выполняющих определенные задачи, такие как автоматизация обслуживания клиентов, имитация человеческого общения в социальных сетях, помощь компаниям в поиске контента в Интернете и в поисковой оптимизации.

Компании и частные лица используют ботов для замены повторяющихся задач, которые в противном случае пришлось бы выполнять людям. Задачи, выполняемые ботами, обычно просты и выполняются гораздо быстрее, чем если бы их делал человек. Однако не все выполняемые ботами задачи безопасны. Иногда ботов используют для преступных действий, таких как кража данных, мошенничество и [DDoS-атаки](https://www.kaspersky.ru/resource-center/threats/ddos-attacks).

**Вредоносные боты и опасности со стороны интернет-ботов**

Вредоносные и интернет-боты могут быть запрограммированы на взлом учетных записей пользователей, поиск контактной информации в интернете, рассылку спама и выполнение других вредоносных действий.

Для проведения таких атак и сокрытия источника атак злоумышленники могут распространять вредоносные боты через [ботнет](https://www.kaspersky.ru/resource-center/threats/botnet-attacks). Ботнет – это несколько подключенных к интернету устройств, на каждом из которых работает один или несколько ботов, часто без ведома владельцев устройств. Каждое устройство имеет собственный IP-адрес, и трафик ботнета поступает с множества IP-адресов. Это затрудняет выявление и блокировку источника вредоносного трафика со стороны ботов. Часто ботнеты растут сами по себе, рассылая с зараженных устройств спам-сообщения, заражающие другие устройства.

Один из наиболее распространенных способов заражения компьютеров ботами – это загрузки. Вредоносные программы доставляются в виде файла загрузки через социальные сети или сообщения электронной почты, в которых рекомендуется перейти по ссылке. Ссылка часто представляет собой изображение или видео, содержащее вирусы и другие вредоносные программы. Компьютер, зараженный вредоносной программой, может стать частью ботнета.

Бот также может отображать предупреждение о том, что компьютер заразится вирусом, если не перейти по соответствующей ссылке, однако именно при переходе по ссылке компьютер заражается вирусом.

Вредоносные боты являются проблемой как для организаций, так и для клиентов. Опасности клиентов включают потенциальную возможность кражи данных и личной информации, перехват нажатий клавиш клавиатуры при вводе конфиденциальной информации, такой как пароли, банковские реквизиты и адреса, а также [фишинг](https://www.kaspersky.ru/resource-center/preemptive-safety/phishing-prevention-tips).

Вредоносные боты легко могут оставаться незамеченными. Они легко скрываются на компьютере и часто их имена файлов и процессов аналогичны или идентичны именам стандартных системных файлов и процессов.

Примеры вредоносных ботов:

**Спам-боты**

Спам-боты могут собирать адреса электронной почты со страниц контактов или гостевых книг. Кроме того, они могут размещать рекламный контент на форумах или в разделах комментариев, чтобы привлечь трафик на определенные сайты.

**Вредоносные чат-боты**

Веб-сайты и приложения служб знакомств – любимое место вредоносных чат-ботов. Эти чат-боты выдают себя за живых людей, подражая реальному человеческому общению. Часто их жертвами становятся пользователи, не осознавшие, что общаются с вредоносными программами, целью которых является получение личной информации, включая номера кредитных карт.

**Боты для обмена файлами**

Эти боты получают от пользователя запрос (например, популярный фильм или музыкальный альбом) и в ответ сообщают, что у них есть доступный для загрузки файл и предоставляют ссылку. Пользователь переходит по ссылке, загружает и открывает ее, и неосознанно заражает свой компьютер.

**Заполнение учетных данных**

Такие боты вводят известные имена пользователей и пароли (обычно получаемые в результате утечки данных) на страницы входа для несанкционированного доступа к учетным записям пользователей.

**DoS и DDoS-боты**

Здесь избыточный трафик со стороны ботов используется специально для создания чрезмерной нагрузки на ресурсы сервера и остановки работы сервисов.

**Атаки на интернет-магазины**

Эти атаки нацелены на интернет-магазины; их цель – отображение товаров как отсутствующих в наличии. При атаках этого типа вредоносные боты получают доступ к корзине покупок, выбирают товары в интернет-магазине и добавляют их в корзину, не завершая покупку. В результате, когда реальный пользователь хочет купить товар, отображается сообщение о том, что товара нет в наличии, хотя фактически товар доступен.

**Поиск уязвимостей**

Боты этого типа проверяют миллионы сайтов на наличие уязвимостей и сообщают об обнаруженных уязвимостях. В отличие от «честных» ботов, которые информируют владельца веб-сайта, вредоносные боты сообщают об обнаруженных уязвимостях своему разработчику, который затем продает ее или использует для взлома.

**Боты для накручивания кликов**

Эти боты создают огромное количество вредоносного трафика, специально нацеленного на платную рекламу с целью мошенничества. Этот мошеннический трафик перехода по платным рекламным объявлениям ежегодно обходится рекламодателям в миллиарды долларов, поскольку часто замаскирован под легальный трафик. Такие действия ботов могут стоить рекламодателям значительную часть их рекламного бюджета, если не используется надежное программное обеспечение для обнаружения ботов.

**Мониторинг трафика**

Эти боты используются для перегрузки почтовых серверов и для крупномасштабных краж данных.

**Зачем злоумышленники используют ботов?**

**1. Для кражи финансовых и персональных данных**

Злоумышленники могут использовать ботнеты для рассылки фишинговых сообщений и для других видов мошенничества, чтобы обманным путем получить деньги пользователей. Они также могут собирать информацию с зараженных ботами машин и использовать ее для кражи личных данных, получения займов на имя пользователя или оплаты покупок от его имени.

**2. Для атак на легальные веб-сервисы**

Злоумышленники могут использовать ботнеты для DoS и DDoS-атак, направляющих на легальный сервис или сеть огромный объем трафика. Такой объем трафика может существенно замедлить работу веб-сервиса или сети компании или создать на них избыточную нагрузку, что приведет к остановке их работы.

**3. Для вымогательства денег**

Злоумышленники получают доход от DoS-атак за счет вымогательства (например, требование от владельцев сайта платы за то, чтобы сайт не был отключен) или платежей со стороны групп, заинтересованных в нанесении ущерба компании или сети. Такие группы включают «хактивистов» — хакеры с определенными политическими взглядами, а также иностранные военные и разведывательные организации.

**4. Для получения денег на системах зомби и ботнетах**

Киберпреступники также могут сдавать ботнеты в аренду другим злоумышленникам для рассылки спама, мошенничества, фишинга, кражи личных данных и атак на легальные веб-сайты и сети.



**Типы ботов**

Что делают боты, не являющиеся вредоносными? Есть много разных видов ботов:

**Чат-боты**

Боты, имитирующие человеческий разговор, отвечают запрограммированными ответами на определенные фразы.

**Социальные боты**

[Боты, работающие в социальных сетях](https://eandt.theiet.org/content/articles/2019/09/social-media-bots-are-becoming-more-human-and-difficult-to-detect-study-shows/), используются для автоматического написания сообщений, отстаивания идей, выступают в качестве подписчиков пользователей и как фиктивные учетные записи для получения подписчиков. По мере усложнения алгоритмов работы социальных сетей, социальным ботам становится все труднее создавать фиктивные учетные записи. Социальных ботов сложно выявить, поскольку они могут вести себя как реальные пользователи.

**Боты для совершения покупок**

Боты, осуществляющие мониторинг цен и выполняющие поиск лучшей цены на продукты, интересные пользователю. Некоторые боты наблюдают шаблоны поведения пользователя при навигации по сайту, а затем настраивают этот сайт для пользователя.

**Боты-пауки или поисковые роботы**

Боты, которые сканируют контент веб-страниц по всему интернету, чтобы помочь Google и другим поисковым системам понять, как оптимально отвечать на поисковые запросы пользователей. Боты-пауки загружают HTML и другие ресурсы, такие как CSS, JavaScript и изображения, и используют их для обработки содержимого сайта.

**Боты для считывания веб-страниц**

Боты, считывающие данные с веб-сайтов с целью сохранения их в автономном режиме для повторного использования. Это может быть считывание как всего содержимого веб-страниц, так и конкретных данных, например, названий и цен продуктов на веб-сайтах электронной коммерции.

В некоторых случаях считывание является законным и разрешено владельцами веб-сайтов. В других случаях боты могут нарушать условия использования веб-сайтов или осуществлять кражу конфиденциальных или защищенных авторским правом материалов.

**Боты-сборщики информации (Knowbots)**

Боты, которые собирают для пользователей информацию, соответствующую определенным критериям, автоматически посещая веб-сайты.

**Боты для мониторинга**

Боты, используемые для мониторинга работоспособности веб-сайта или системы. Например, Downdetector.com – независимый сайт, в реальном времени предоставляющий информацию о статусе веб-сайтов и сервисов, включая данные о сбоях.

**Транзакционные боты**

Такие боты используются для совершения транзакций от имени людей. Например, транзакционные боты позволяют клиентам совершать транзакции в контексте разговора.

**Боты-загрузчики**

Боты, используемые для автоматической загрузки программного обеспечения или мобильных приложений. Они используются для управления статистикой загрузок, например, чтобы увеличить количество загрузок в популярных магазинах приложений и помочь новым приложениям подняться в верхние строки поиска.

Однако также их можно использовать для атак на сайты загрузки, создавая поддельные загрузки как часть DoS-атак (отказ в обслуживании).

**Билетные боты**

[Боты, которые автоматически покупают билеты на популярные мероприятия](https://www.theregister.com/2019/03/01/ticket_scalper_bots/) для перепродажи с целью получения прибыли. Эта деятельность является незаконной во многих странах. Даже если она напрямую не противоречит закону, она причиняет неудобства организаторам мероприятий, легальным продавцам билетов и потребителям. Часто билетные боты бывают непростыми, они имитируют поведение реальных покупателей билетов.

**Как работают боты?**

Обычно боты работают по сети. Боты, которые могут взаимодействовать друг с другом, используют для этого интернет-сервисы: обмен мгновенными сообщениями, интерфейсы, такие как Twitterbots, или ретранслируемый интернет-чат (Internet Relay Chat, IRC).

Боты представляют собой набор алгоритмов для выполнения определенных задач. Различные типы ботов разработаны для выполнения разных задач.

В качестве примера разберем чат-ботов и рассмотрим разные методы их работы:

* **Чат-бот на основе правил** при взаимодействии с пользователями предоставляет им выбор заранее определенных опций.
* **Интеллектуально независимый чат-бот** использует машинное обучение на основе вводимых пользователями данных, а также ищет известные ключевые слова.
* **Чат-боты с искусственным интеллектом** представляют собой комбинацию чат-ботов на основе правил и интеллектуально независимых чат-ботов. Кроме того, эти чат-боты могут выполнять сравнение с шаблоном, обработку выражений естественного языка и инструменты генерации выражений естественного языка.

У каждого вида ботов есть свои плюсы и минусы. Компании, использующие ботов, выбирают наиболее подходящий вид, исходя из своих требований.

**Плюсы и минусы ботов**

**Плюсы компьютерных и интернет-ботов:**

* Быстрее людей выполняют повторяющиеся задачи.
* Экономят время клиентов и покупателей.
* Снижают затраты на рабочую силу для организаций.
* Доступны круглосуточно (24/7).
* Приложения для обмена сообщениями позволяют компаниям общаться с большим количеством людей.
* Настраиваемые.
* Многоцелевые.
* Боты могут оптимизировать пользовательский интерфейс.

**Минусы компьютерных и интернет-ботов:**

* Ботов нельзя настроить для выполнения определенных задач, в которых есть риск неправильно понять пользователей и вызвать у них разочарование в процессе.
* Для управления ботами по-прежнему требуются люди. Также участие человека необходимо в случае возникновения непонимания.
* Боты могут быть запрограммированы на совершение вредоносных действий.
* Ботов можно использовать для рассылки спама.

**Примеры ботов**

Множество и разнообразие ботов позволяет использовать их в самых разных областях, таких как обслуживание клиентов, бизнес, поиск и развлечения.

Примеры известных сервисов, использующих ботов:

* Приложения для обмена мгновенными сообщениями, такие как Facebook Messenger, WhatsApp и Slack.
* Чат-боты, такие как Google Assistant и Siri.
* Всемирная организация здравоохранения [создала в WhatsApp бота](https://www.who.int/news-room/feature-stories/detail/who-health-alert-brings-covid-19-facts-to-billions-via-whatsapp) для распространения публичной информации, связанной с пандемией коронавируса.
* Для продвижения шоу Genius National Geographic разработало приложение для общения, которое якобы общалось в стиле Альберта Эйнштейна.
* Новостные приложения, такие как Wall Street Journal, для отображения заголовков новостей.
* Spotify – позволяет пользователям искать и обмениваться треками через Facebook Messenger.
* Lyft – основной конкурент Uber, позволяет клиентам отправлять запросы через Slack, Messenger и Alexa.
* Mastercard позволяет клиентам проверять транзакции по счетам с помощью бота Facebook Messenger.
* Компания Lidl создала [бота, помогающего давать клиентам рекомендации по винам](https://chatbotsmagazine.com/how-we-built-the-wine-bot-margot-for-lidl-b54f42cda4dd?gi=af3a971f883c).

**Как выяснить, заражен ли компьютер ботами**

Существуют следующие способы определить, является ли компьютер частью ботнета:

* Происходят сбои в работе компьютера без видимой причины.
* Приложения, которые раньше работали без сбоев, теперь работают с перебоями.
* Программы, которые раньше загружались быстро, теперь запускаются медленно.
* Компьютер долго не выключается или не выключается должным образом.
* Доступ в Интернет существенно замедляется.
* В браузере появились компоненты, которые вы не загружали.
* В диспетчере задач Windows появились программы с непонятными названиями и описаниями.
* Изменились настройки, и нет возможность вернуть их к предыдущим значениям.
* Появляются всплывающие окна и рекламные объявления, даже если не используется веб-браузер.
* Повышается скорость работы вентилятора, когда устройство не используется.
* Вам сообщают, что получили от вас сообщения электронной почты, которые вы не отправляли.
* Не удается загрузить обновления операционной системы.

**Что делать, если компьютер заражен ботами**

Если компьютер уже заражен ботами, самое важное – защитить данные.

Несколько предпринять следующие шаги:

**Шаг 1.** Отключите компьютер от сети как можно скорее – это остановит кражу конфиденциальных данных и помешает использованию компьютера для атак на другие сети.

**Шаг 2.** Перенесите все важные и личные данные на другой компьютер или внешний жесткий диск. Однако сначала убедитесь, что на этих устройствах нет вредоносных программ.

**Шаг 3.** Выполните сброс настроек компьютера до заводских (имейте в виду, что помимо решения проблемы это действие также повлечет удаление созданных вами файлов и программ, драйверов, и будет выполнен возврат настроек к значениям по умолчанию).

**Шаг 4.** Очистите компьютер с помощью различных инструментов безопасности или обратитесь к специалисту.

Помните, что профилактика – лучшее средство против ботов и других видов вредоносных программ. Поэтому важно, чтобы на всех ваших устройствах были установлены программы обеспечения кибербезопасности.

**Как защитить компьютер от ботов**

Сложность заключается в том, что многие точки контакта с клиентами в интернете, включая веб-сайты, мобильные приложения и API-интерфейсы, подвергаются атакам со стороны ботов. Защитить компьютер от ботов возможно, но это требует бдительности и понимания того, что именно искать.

Ниже приведено несколько действий, необходимых для защиты систем от проникновения ботнетов:

**Установите антивирусное программное обеспечение**

Используйте комплексное антивирусное программное обеспечение для защиты устройства. Например, [Kaspersky Total Security](https://www.kaspersky.ru/total-security) блокирует вирусы и вредоносные программы в режиме реального времени и не позволяет злоумышленникам удаленно захватить ваш компьютер. Убедитесь, для антивирусных и антишпионских программ настроено автоматическое обновление.

**Убедитесь, что обновлены все программы**

Никогда не пропускайте обновления системы. Регулярно проверяйте наличие обновлений и исправлений для браузера и операционной системы.

**Используйте надежный пароль**

Надежный пароль сложно подобрать, он состоит из комбинации заглавных и строчных букв, цифр и символов. Не следует использовать один и тот же пароль для нескольких учетных записей. Рекомендуется использовать надежный [менеджер паролей](https://www.kaspersky.ru/password-manager).

**Переходите только по доверенным ссылкам**

Переходите по ссылкам в интернете или открывайте сообщения электронной почты, только если вы доверяете их источникам. Опасность обычно возникает при загрузке контента с неизвестных сайтов или получении его от людей, не использующих современные средства защиты и непреднамеренно распространяющих зараженные файлы.

Всегда будьте предельно осторожны при загрузке данных и файлов от лиц, чей компьютер не защищен. Старайтесь не использовать флэш-накопители на зараженном компьютере.

**Избегайте ненадежных веб-сайтов и рекламы**

Обычно пользователи загружают вредоносных ботов, когда им при просмотре веб-страниц попадается интригующая реклама или загрузка. Будьте осторожны при загрузке бесплатных версий программного обеспечения с незнакомых веб-сайтов и никогда не нажимайте на всплывающие объявления с предложением повысить производительность компьютера или решить проблемы с вирусами. В большинстве случаев взаимодействие с этими страницами приводит к установке вредоносных программ на компьютер.

**Установите сетевой экран**

[Сетевой экран](https://www.kaspersky.ru/resource-center/definitions/firewall) помогает блокировать вредоносные атаки.

**Используйте менеджер ботов**

Менеджер ботов позволяет остановить вредоносных ботов. Менеджеры ботов могут входить в состав платформы по обеспечению безопасности веб-приложений.

Менеджер ботов позволяет разрешить использование одних ботов и заблокировать использование других, потенциально опасных для системы. Для этого он классифицирует все входящие запросы от людей и «хороших» ботов, а также от известных вредоносных и неизвестных ботов. Затем менеджер ботов направляет весь подозрительный трафик со стороны ботов с сайта.

Некоторые базовые наборы функций управления ботами включают ограничение скорости для IP-адресов и контрольное изображение CAPTCHA. Ограничение скорости для IP-адресов позволяет ограничить количество запросов с одних и тех же адресов, а CAPTCHA часто используется, чтобы отличить ботов от людей с помощью ввода кода с картинки.

«Хорошие» боты являются важной частью инфраструктуры интернета и выполняют множество полезных задач. Вредоносных ботов трудно обнаружить без [антивирусной программы](https://www.kaspersky.ru/antivirus), потому что они спрятаны на видном месте. Таким образом, важно осознавать риски со стороны вредоносных ботов и всегда поддерживать надлежащий уровень кибербезопасности.

**https://www.kaspersky.ru/resource-center/definitions/what-are-bots**