**Угроза информационной безопасности** — совокупность условий и факторов, создающих опасность нарушения [информационной безопасности](https://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C).

Под угрозой (в общем) понимается потенциально возможное событие, действие (воздействие), процесс или явление, которые могут привести к нанесению ущерба чьим-либо интересам.

Угрозы информационной безопасности могут быть классифицированы по различным признакам:

* По аспекту информационной безопасности, на который направлены угрозы:

*Угрозы*[*конфиденциальности*](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BD%D1%84%D0%B8%D0%B4%D0%B5%D0%BD%D1%86%D0%B8%D0%B0%D0%BB%D1%8C%D0%BD%D0%BE%D1%81%D1%82%D1%8C) (неправомерный доступ к информации). Угроза нарушения конфиденциальности заключается в том, что информация становится известной тому, кто не располагает полномочиями доступа к ней. Она имеет место, когда получен доступ к некоторой информации ограниченного доступа, хранящейся в вычислительной системе или передаваемой от одной системы к другой. В связи с угрозой нарушения конфиденциальности, используется термин «утечка».

Подобные угрозы могут возникать вследствие «человеческого фактора» (например, случайное делегировании тому или иному пользователю привилегий другого пользователя), сбоев работе программных и аппаратных средств.

К информации ограниченного доступа относится государственная тайна и конфиденциальная информации (коммерческая тайна, персональные данные, профессиональные виды тайна: врачебная, адвокатская, банковская, служебная, нотариальная, тайна страхования, следствия и судопроизводства, переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений (тайна связи), сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации (ноу-хау) и др.).

* + *Угрозы*[*целостности*](https://ru.wikipedia.org/wiki/%D0%A6%D0%B5%D0%BB%D0%BE%D1%81%D1%82%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%B8) (неправомерное изменение данных). Угрозы нарушения целостности – это угрозы, связанные с вероятностью модификации той или иной информации, хранящейся в информационной системе. Нарушение целостности может быть вызвано различными факторами – от умышленных действий персонала до выхода из строя оборудования.
  + *Угрозы*[*доступности*](https://ru.wikipedia.org/wiki/%D0%94%D0%BE%D1%81%D1%82%D1%83%D0%BF%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%B8) (осуществление действий, делающих невозможным или затрудняющих доступ к ресурсам информационной системы). Нарушение доступности представляет собой создание таких условий, при которых доступ к услуге или информации будет либо заблокирован, либо возможен за время, которое не обеспечит выполнение тех или иных бизнес-целей.

**Вредоносное ПО**

[*Вредоносное программное обеспечение*](https://blog.malwarebytes.com/glossary/malware/) (или вредоносное ПО) – это собирательный термин, обозначающий вредоносную программу или код, который может причинить ущерб компьютерной системе.

*Цель вредоносного ПО* – получение незаконной прибыли.

Несмотря на то что вредоносное ПО не может повредить аппаратное обеспечение системы или сетевое оборудование, оно может похитить, зашифровать или удалить данные, изменить функции компьютера или перехватить контроль над ними. Кроме того, оно может следить за активностью компьютера.

*Как понять, что система заражена вредоносным ПО?*

[Распространенные признаки наличия](https://blog.malwarebytes.com/101/2016/05/how-to-tell-if-youre-infected-with-malware/) вредоносного ПО в системе:

1. Компьютер начинает работать медленно. Одно из основных последствий проникновения вредоносного ПО в операционную систему – снижение скорости ее работы независимо от того, просматриваете ли Вы веб-страницы или используете локальные приложения.
2. На экране начинает периодически появляться навязчивая реклама. Неожиданные всплывающие рекламные сообщения являются типичным признаком заражения компьютера вредоносным ПО. Чаще всего они вызваны особой формой вредоносного ПО – [рекламным ПО](https://ru.malwarebytes.com/adware/). Всплывающие рекламные блоки обычно связаны с другими скрытыми угрозами со стороны вредоносного ПО.
3. Компьютер часто выдает сбои, «зависает» или отображает «синий экран смерти», который в системах Windows свидетельствует о наличии критической ошибки.
4. По непонятным причинам уменьшилось количество свободного места на диске. Возможно, винить в этом следует разросшееся вредоносное ПО, которое скрывается где-то на жестком диске.
5. Интернет-активность системы странным образом возросла.
6. Интенсивность использования системных ресурсов чрезмерно высока, а охлаждающий вентилятор компьютера постоянно работает на полной скорости. Это верный признак того, что вредоносное ПО использует системные ресурсы в фоновом режиме.
7. Начальная страница браузера изменена. Нажатие на ту или иную ссылку переводит на нежелательные веб-страницы. В аналогичных случаях работа браузера может значительно замедлиться.
8. В браузере внезапно появляются новые панели инструментов, расширения или плагины.
9. Антивирусная программа перестает работать, не удается ее обновить
10. Бывают и очевидные атаки вирусов, которые даже не пытаются маскироваться. Такую тактику выбирают [программы-вымогатели](https://ru.malwarebytes.com/ransomware/): они заявляют о себе, сообщают о том, что похитили Ваши данные, а затем требуют выкуп за возврат файлов.
11. И даже если система как будто в порядке, это еще не повод для самоуспокоения, поскольку отсутствие новостей – далеко не всегда хорошая новость. Опасное вредоносное ПО может спрятаться в недрах компьютера и делать свое грязное дело, не привлекая внимания: похищать пароли, файлы с конфиденциальными данными или использовать Ваш ПК для заражения других компьютеров.

*Как атакует вредоносное ПО?*

Атака вредоносного ПО может осуществляться множеством способов. Самые распространенные пути проникновения вредоносного ПО в систему – через Интернет и через электронную почту. То есть это может случиться в любое время, когда Вы работаете онлайн.

Вредоносное ПО может проникнуть, когда:

- просмотр взломанных веб –сайтов;

-демонстрационные версии игр;

загружаете зараженные музыкальные файлы,

устанавливаете новые панели инструментов незнакомого производителя,

загружаете программы из непроверенных источников,

открываете вложения вредоносных сообщений электронной почты.

Вредоносные объекты часто скрываются в обычных на первый взгляд программах – и вероятность этого возрастает в том случае, если загружаете их не через надежный магазин приложений, а с веб-сайтов или через сообщения. Во время установки приложений важно обращать внимание на предупреждающие сообщения, особенно если они запрашивают разрешение на доступ к Вашей электронной почте или другим персональным данным.

Наилучший способ уберечь себя от опасностей – устанавливать мобильные приложения только из проверенных источников, доверять только надежным сторонним производителям приложений, а также всегда загружать программы непосредственно с веб-сайта производителя – и никогда с других веб-сайтов.

Коварные планы вредоносного ПО не были бы столь успешны без самой важной составляющей – ***Вас***. Они используют Вашу доверчивость, Вашу привычку открывать сообщения электронной почты и переходить к вложениям, которые только выглядят безобидными, они эксплуатируют Ваше желание скорей нажать на ссылку и установить программу, источнику которой на самом деле нельзя доверять. Важно понимать, что мы ни в коем случае не хотим пристыдить Вас, поскольку злоумышленники могут обхитрить даже самых опытных пользователей и заставить их установить вредоносное ПО.

Даже если Вы устанавливаете программу из надежного источника, Вы можете не обратить внимание на то, что она запрашивает разрешение на установку еще одного приложения, которое Вы не собирались устанавливать. Эта дополнительная программа часто замаскирована под важный компонент, которым она часто не является.

Применение еще одного метода, использующего ресурсы [социальной инженерии](https://blog.malwarebytes.com/glossary/social-engineering/), наблюдалось экспертами Malwarebytes в Великобритании. Злоумышленники атаковали пользователей за счет [функции прямого платежа](http://www.theregister.co.uk/2015/08/11/direct_to_bill_mobile_payment_scam/), распространенной в мобильных устройствах. Посещая определенные веб-сайты, пользователи непреднамеренно нажимали на невидимые кнопки, после чего злоумышленники, зная телефонные номера жертв, выставляли им счета прямо через мобильную сеть и успешно списывали средства в свою пользу.

Будем честными: атака вредоносного ПО может быть настолько искусной, что ее невозможно заметить. Велика вероятность, что даже простое посещение вредоносного веб-сайта и просмотр его страницы и/или рекламного баннера приводят к [теневой загрузке нежелательных объектов](https://blog.malwarebytes.com/glossary/drive-by-download/).

С другой стороны, если Вы не используете надлежащую защитную программу, то заражение вредоносным ПО и его последствия остаются целиком на Вашей совести.

*Наиболее распространенные формы вредоносного ПО?*

1. [Рекламное ПО](https://ru.malwarebytes.com/adware/) – это нежелательная программа, написанная для того, чтобы забрасывать экран компьютера рекламными сообщениями (чаще всего во время использования браузера). Как правило, подобные объекты используют мошеннические методы, чтобы принудить пользователя установить их на свой ПК, планшетный компьютер или мобильное устройство: они выдают себя за обычные программы или проникают в систему в качестве «дополнительной нагрузки» при установке других приложений.
2. [Шпионские программы](https://ru.malwarebytes.com/spyware/) – это вредоносное ПО, которое скрытно наблюдает за действиями пользователя компьютера и пересылает накопленные данные своим разработчикам.
3. [Вирусы](https://blog.malwarebytes.com/glossary/virus/) – это вредоносное ПО, которое прикрепляется к другой программе и при ее запуске начинает самовоспроизводиться и модифицировать другие приложения на компьютере, внедряя в них элементы своего вредоносного кода.
4. [Черви](https://blog.malwarebytes.com/glossary/worm/) – это тип вредоносного ПО, напоминающий вирусы. Они также обладают способностью к самокопированию, проникают на компьютер через сеть и обычно наносят вред, удаляя данные или файлы.
5. [Троянские программы](https://blog.malwarebytes.com/glossary/trojan/), также обозначаемые как вредоносные программы типа «троянский конь», – это один из самых опасных типов вредоносного ПО. Они обычно стремятся обмануть, маскируясь под полезные программы. После того как троянская программа проникла в систему, злоумышленники получают несанкционированный доступ к зараженному компьютеру. Троянские программы используются для похищения финансовой информации, а также для того, чтобы проторить дорогу другим вредоносным объектам, например, вирусам и программам-вымогателям.
6. [Программы-вымогатели](https://ru.malwarebytes.com/ransomware/) – это вредоносное ПО, которое блокирует устройство и/или шифрует файлы, а затем заставляет заплатить выкуп за их возврат. Программы-вымогатели считаются излюбленным оружием киберпреступников, поскольку они дают им возможность быстро получить значительную прибыль в [криптовалюте](https://blog.malwarebytes.com/101/2017/11/cryptocurrency-works-cybercriminals-love/" \t "_blank), операции с которой сложно отследить. Код, на котором основываются программы-вымогатели, можно без проблем получить на черном интернет-рынке, а защититься от него всегда непросто.
7. [Руткиты](https://blog.malwarebytes.com/glossary/rootkit/) – это вредоносное ПО, которое предоставляет злоумышленникам права администратора на зараженном компьютере. Обычно они остаются незамеченными для пользователя, других программ и самой операционной системы.
8. [Клавиатурные шпионы](https://blog.malwarebytes.com/glossary/keylogger/) – это вредоносное ПО, которое записывает, на какие клавиши нажимают пользователи, сохраняет накопленную информацию и отправляет ее своим авторам, которые извлекают из полученных данных важные сведения, например имена пользователей, пароли или реквизиты кредитных карт.
9. [Программы для теневого вредоносного майнинга](https://blog.malwarebytes.com/101/2018/02/how-to-protect-your-computer-from-malicious-cryptomining/), также иногда обозначаемые как [программы для криптоджекинга](https://ru.malwarebytes.com/cryptojacking/), – это тип вредоносного ПО, который получает все более широкое распространение. Эти объекты используются для скрытого майнинга криптовалют и обычно устанавливаются с помощью троянской программы. В результате посторонние лица могут использовать ресурсы компьютера, чтобы добывать криптовалюты, например биткоин или монеро. Не давая зарабатывать деньги на мощности своего компьютера, криптомайнеры отправляют полученные «монеты» на собственные счета. Программы для вредоносного майнинга фактически крадут ресурсы чужих систем с целью получения прибыли.
10. [Эксплойты](https://blog.malwarebytes.com/glossary/exploit/) – это вредоносное ПО, которое использует ошибки и [уязвимости](https://blog.malwarebytes.com/glossary/software-vulnerability/) в системе, чтобы передать своим авторам контроль над ней. Как и другие угрозы, эксплойты нередко распространяются через [вредоносную рекламу](https://blog.malwarebytes.com/101/2016/06/truth-in-malvertising-how-to-beat-bad-ads/): она может отображаться даже на обычных веб-сайтах, которые извлекают вредоносный контент из скомпрометированных веб-сайтов. В случае успешной атаки эксплойт пытается проникнуть в систему посредством теневой загрузки. Пользователю даже не приходится нажимать на кнопку. Достаточно просто посетить вполне благонадежный веб-сайт в неудачный день.

### *Краткая история развития вредоносного ПО*

**1980-е годы**: Теоретическое осмысление «самовоспроизводящихся автоматов» (т. е. вирусов) было сформулировано в статье, увидевшей свет в 1949 году. Самые ранние вирусы стали появляться в 1970-х годах на платформах, предшествующих персональным компьютерам. Вместе с тем, история современных вирусов начинается с программы Elk Cloner, которая поразила системы Apple II в 1982 году. Этот вирус, переносчиком которого были зараженные дискеты, не причинял никакого вреда, однако он проникал на все носители, подключаемые к системе, и распространялся столь стремительно, что данный случай действительно можно считать первой в истории крупномасштабной эпидемией компьютерного вируса. Обратите внимание: это произошло задолго до появления вредоносного ПО для Windows. Впоследствии вирусы и черви получили широкое распространение.

**1990-е годы**: Это десятилетие проходило под знаком становления платформы Microsoft Windows; в ее приложениях активно использовались гибкие макросы, которые позволяли злоумышленникам писать вредоносный код на макроязыке Microsoft Word и других программ. Эти макровирусы поражали документы и шаблоны намного чаще, чем исполняемые приложения, хотя, строго говоря, макросы документа Word сами являются одной из форм исполняемого кода.

**2002–2007 годы**: Черви интернет-пейджеров – образцы самовоспроизводящегося вредоносного кода, которые передаются через сети обмена мгновенными сообщениями – получили обширное распространение, используя слабые места в защите таких сетей, как AOL AIM, MSN Messenger и Yahoo Messenger, а также поражая корпоративные системы обмена мгновенными сообщениями.

**2005–2009 годы**: Частыми стали атаки рекламного ПО, представляющего собой нежелательную рекламу на экране компьютера – иногда в форме всплывающего окна, которое невозможно было закрыть. Для распространения эти вредоносные объекты нередко эксплуатировали уязвимости законных программ, однако ближе к 2008 году сами издатели программного обеспечения начали использовать рекламные компании в мошеннических целях. Это привело к многомиллионным штрафам. В результате компании, занимавшиеся разработкой рекламного ПО, вынуждены были прекратить работу.

**2007–2009 годы**: Авторы вредоносного ПО обратили свое внимание на социальные сети, например MySpace, рассматривая их как удобную среду для мошеннической рекламы, перенаправлений, ложных антивирусов и фиктивных средств защиты. Их уловки основывались на методах социальной инженерии. Со временем популярность сети MySpace пошла на спад и излюбленными платформами злоумышленников стали Facebook и Twitter. Здесь также использовались опробованные тактики, в том числе подставные ссылки на [фишинговые](https://blog.malwarebytes.com/glossary/phishing/" \t "_blank) страницы и реклама приложений для Facebook с вредоносными расширениями. Когда и эти способы стали малоэффективными, [мошенники быстро освоили новые методы кражи](https://blog.malwarebytes.com/tech-support-scams/).

**2013 год**: Новой формой вредоносного ПО стали программы-вымогатели. В числе первых была программа CryptoLocker, действовавшая с сентября 2013 года до конца мая 2014 года. Ее основными целями были компьютеры под управлением Windows. Пользователи, чьи системы стали жертвами CryptoLocker, вынуждены были выплатить около 27 миллионов долларов – и это только за последний квартал 2013 года. Успех этой программы-вымогателя привел к всплеску активности других программ с похожим именем. Одному из таких имитаторов удалость выманить всего у 1000 потерпевших 18 миллионов долларов с апреля 2014 года по июнь 2015 года.

**2013–2017 годы**: Освоив методы доставки с помощью троянских программ, эксплойтов и вредоносной рекламы, программы-вымогатели стали настоящим «королем» вредоносного ПО. Особо крупные вспышки заражения в 2017 году затронули множество предприятий в самых различных отраслях. Действия программы-вымогателя до предела просты: сначала она шифрует данные своей жертвы, а затем требует выкуп за возврат доступа к ним.

**2017 год – настоящее время**: Криптовалюты и методы их добычи – вот что захватило умы многих людей по всему миру и привело к появлению нового типа вредоносного ПО – программ для криптоджекинга, которые скрытно используют ресурсы чужого устройства с целью майнинга криптовалюты.

*Поражает ли вредоносное ПО компьютеры Mac?*

Бытует мнение, что [устройства Mac и iPad невосприимчивы к вирусам](https://blog.malwarebytes.com/101/2017/03/mac-security-facts-and-fallacies/) (и поэтому не нуждаются в [антивирусных программах](https://ru.malwarebytes.com/mac-antivirus/)). В целом, это правда. По крайней мере, в прошлом наблюдались длительные периоды затишья.

На эти системы нацелены другие типы вредоносного ПО – и это предмет отдельного разговора. Системы Mac имеют те же уязвимости (и связанные с ними симптомы заражения), что и компьютеры под управлением Windows, так что их надежность в этом отношении не абсолютна. Так, встроенная защита Mac от вредоносного ПО не может заблокировать все рекламное ПО и все шпионские программы, которые проникают на компьютер вместе с загружаемыми мошенническими программами. Троянские программы и клавиатурные шпионы также представляют угрозу. Программа-вымогатель, написанная специально для системы Mac, была обнаружена в марте 2016 года, когда атака на основе троянской программы затронула более 7000 компьютеров Mac.

Примечательно, что продукты Malwarebytes зафиксировали в 2017 году больше вредоносного ПО для систем Mac, чем в любой предыдущий год. К концу 2017 года количество новых уникальных угроз, подсчитанных на платформе Mac нашими специалистами, выросло на 270 процентов по сравнению с 2016 годом.

Чтобы посетить блог Malwarebytes и ознакомиться с дополнительной информацией о вредоносном ПО для Mac, пожалуйста, нажмите [здесь](https://blog.malwarebytes.com/101/2018/03/the-state-of-mac-malware/).

*Поражает ли вредоносное ПО мобильные устройства?*

Киберпреступники и производители вредоносного ПО отлично себя чувствуют на рынке мобильных устройств. Ведь смартфоны в действительности являются портативными компьютерами со множеством функций. Кроме того, они представляют собой сокровищницу персональных данных, финансовой информации и других ценных сведений, которые привлекают желающих заработать деньги нечестным путем.

К сожалению, почти экспоненциальный рост количества смартфонов повлек за собой всплеск активности вредоносных программ, пытающихся воспользоваться уязвимостями этих устройств.

Рекламное ПО, троянские программы, шпионские программы, черви и программы-вымогатели – все эти вредоносные объекты могут проникнуть на Ваш телефон самыми различными способами.

Переход по рискованной ссылке или загрузка непроверенного приложения – лишь самые очевидные источники проблем. Однако Вы также можете заразить телефон через электронную почту, тексты или даже через подключение Bluetooth. Кроме того, некоторые типы вредоносного ПО, например черви, распространяются непосредственно с одного телефона на другой.

Словом, это крупный рынок (и крупная цель). Согласно [одному из источников статистики](http://www.itnewsafrica.com/2018/03/meet-the-hackers-a-series-on-mobile-malware/) в мире насчитывается 2,1 миллиарда пользователей мобильных устройств, а к 2019 году ожидается рост до 2,5 миллиарда. Каждый четвертый пользователь имеет больше одного устройства. Поэтому злоумышленники считают рынок мобильных устройств чрезвычайно привлекательной целью, ведь принцип повышения эффективности «производства» за счет роста его масштабов позволяет им получать баснословные прибыли при минимальных затратах.

Кроме того, атаковать пользователей мобильных устройств может быть намного проще. В большинстве случаев они [не защищают свои телефоны](https://blog.malwarebytes.com/101/2016/09/top-10-ways-to-secure-your-mobile-phone/) так же надежно, как и компьютеры, не устанавливают защитные программы или вовремя не обновляют операционную систему. Это делает их уязвимыми даже для примитивного вредоносного ПО. Экраны мобильных устройств невелики, и пользователь просто не в состоянии уследить за всем, что происходит в системе. Подозрительная активность, которая в условиях ПК обычно свидетельствует об атаке вируса, может остаться незамеченной, как в случае со шпионскими программами.

Зараженные мобильные устройства еще опасней зараженных ПК. Взломав смартфон, злодеи могут следить за каждым Вашим шагом с помощью камеры, подслушивать разговоры. Что еще хуже, вредоносное ПО, нацеленное на мобильный банкинг, перехватывает входящие звонки и текстовые сообщения, чтобы обойти двухступенчатую авторизацию, используемую многими банковскими приложениями.

«Более популярная платформа Android привлекает намного больше вредоносного ПО, чем iPhone».

Важно помнить, что дешевые телефоны могут продаваться с уже предустановленным вредоносным ПО, которое практически невозможно удалить.

В среде вредоносного ПО для мобильных устройств наиболее распространены объекты, поражающие две основные операционные системы – Android от Google и iOS от Apple. Android лидирует на рынке – с этой операционной системой продается 80 процентов всех смартфонов; доля iOS составляет 15 процентов. Поэтому нет ничего удивительного в том, что более популярная платформа Android привлекает намного больше вредоносного ПО, чем iPhone. Давайте рассмотрим каждую из них в отдельности.

*Как понять, что устройство Android заражено вредоносным ПО?*

К счастью, есть несколько признаков, по которым можно безошибочно определить, что устройство Android подверглось заражению. Итак, Вы были атакованы, если замечаете следующее:

* Внезапное появление всплывающих окон с навязчивой рекламой. Если они появляются из ниоткуда и направляют Вас на схематично оформленные веб-сайты, то Вы, вероятно, установили приложение, в котором скрыто рекламное ПО. Поэтому не нажимайте на рекламный блок.
* Странный всплеск использования данных. Вредоносное ПО может расходовать значительные части Вашего тарифного плана, чтобы отображать рекламу и отправлять злоумышленникам похищенную на телефоне информацию.
* Подозрительные суммы в выставленных к оплате счетах. Такое случается, когда вредоносное ПО совершает звонки и отправляет текстовые сообщения на платные номера.
* Быстро исчезающий заряд аккумулятора. Вредоносное ПО потребляет ресурсы телефона и, соответственно, быстрее разряжает аккумулятор.
* Абоненты из Вашего списка контактов сообщают о странных звонках и текстовых сообщениях, поступающих с Вашего телефона. Вредоносное ПО самовоспроизводится, оправляя свои копии с одного устройства на другое по электронной почте и даже в текстовых сообщениях, предлагающих другим пользователям перейти по специальной ссылке.
* Перегрев телефона при одновременном снижении его производительности. Существует, например, троянская программа, которая проникает в систему Android и приносит за собой крайне агрессивный установщик; он в свою очередь перегружает процессор, вызывает чрезмерный нагрев телефона и истощает аккумулятор (иногда даже вызывая его деформацию), что, разумеется, [приводит устройство Android в полную негодность](https://blog.malwarebytes.com/cybercrime/2017/12/lo-lo-lo-lo-loapi-we-have-you-protected/).
* Неожиданные приложения на экране. Иногда вредоносные программы скрытно проникают в систему в качестве «дополнительной нагрузки» при установке других приложений. Это происходит из-за того, что Android позволяет переходить напрямую из Google Play в другой магазин, например Amazon, который мог упустить тот или иной вредоносный объект.
* Телефон сам включает Wi-Fi и мобильный Интернет. Это еще один способ распространения вредоносного ПО, когда оно игнорирует Ваши настройки и открывает каналы для заражения.
* Ниже мы расскажем Вам о том, что следует предпринять, если [на Ваше устройство Android все-таки проник вирус](https://blog.malwarebytes.com/101/2018/03/10-ways-to-protect-your-android-phone/). Также рекомендуем Вам прочитать статью в блоге Malwarebytes, посвященную [защите персональных данных на устройствах Android](https://blog.malwarebytes.com/cybercrime/2017/04/mobile-menace-monday-securing-your-privacy-on-android/).

*Как понять, что iPhone или iPad заражены вредоносным ПО?*

Если название Вашего смартфона начинается с маленькой буквы «i», похвалите себя за этот выбор, поскольку вредоносное ПО не является столь острой проблемой для iPhone. Нельзя сказать, что его не существует, но оно встречается крайне редко. Обычно вредоносное ПО может проникнуть на iPhone только в двух случаях, которые сами по себе являются экстраординарными.

«Несмотря на то что открытая атака вредоносного ПО маловероятна, использование iPhone не защитит Вас от мошеннических звонков и текстовых сообщений».

Первый случай предполагает целевую атаку злоумышленников на национальном уровне – государственные структуры могут создать или купить (за многие миллионы долларов) вредоносное ПО, способное воспользоваться некоторыми уязвимостями в iOS. И здесь не стоит удивляться, поскольку в любом устройстве есть уязвимость. Нужно отдать должное компании Apple, которая проделала отличную работу по обеспечению безопасности iOS, где ни одно приложение (в том числе и защитные программы) не может сканировать телефон или другие приложения, установленные в системе. Именно поэтому разработка подобного вредоносного ПО, способного проникнуть в систему и удаленно выполнять какие-либо операции, обходится крайне дорого.

[Очень примечательная история](http://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/) произошла в 2016 году, когда на iPhone представителя известной организации по защите прав человека, расположенной в Объединенные Арабских Эмиратах (ОАЭ), пришло текстовое SMS-сообщение с обещанием раскрыть «новые секреты» о пытках заключенных в тюрьмах ОАЭ. Получателю предлагалось перейти по прилагаемой ссылке. Он не стал этого делать, а отправил сообщение специалистам в области кибербезопасности, которые изучили текст и обнаружили эксплойт, способный превратить телефон жертвы в настоящего цифрового шпиона.

Второй случай предполагает, что пользователь сам делает iPhone уязвимым за счет взлома (джейлбрейка), который снимает ограничения, наложенные компанией Apple на использование телефона, – в первую очередь это касается запрета на установку приложений не из магазина App Store. Компания Apple тщательно проверяет представленных в нем разработчиков и накладывает на них санкции даже в том случае, если вредоносному ПО удается пробраться в систему вслед за обычным приложением.

И еще. Несмотря на то что открытая атака вредоносного ПО маловероятна, использование iPhone не защитит Вас от мошеннических звонков и текстовых сообщений. Если Вы нажмете на ссылку в сообщении, полученном от неизвестного отправителя (или от пользователя, который выдает себя за другого), то Вы можете попасть на мошеннический сайт, где Вам предложат ввести свой пароль или другие личные данные. Так что не нужно недооценивать изобретательность киберпреступников. Всегда действуйте осторожно.

*Кого атакует вредоносное ПО?*

Ответ прост: кого угодно. В мире миллиарды устройств, принадлежащих частным пользователям. С их помощью люди совершают банковские операции, покупки в розничных магазинах, а также передают и сохраняют самую разную информацию, которую кое-кто не прочь похитить. Для злоумышленников мобильные устройства – лишь среда распространения рекламного ПО, шпионских программ, клавиатурных шпионов и вредоносной рекламы. Поэтому они стремятся создавать новые виды вредоносных объектов и доставлять как можно больше их копий на различные устройства, прилагая для этого по возможности минимум усилий.

«Если Вы используете свой смартфон или планшетный компьютер на рабочем месте, хакеры могут атаковать организацию Вашего работодателя».

Криптомайнеры и распространители программ-вымогателей одинаково опасны для своих целей. Их жертвами становятся не только частные лица, но и целые предприятия, больницы, муниципальные учреждения и магазины розничной торговли.

Потребители являются не единственной целью злоумышленников, создающих шпионские программы. Если Вы используете свой смартфон или планшетный компьютер на рабочем месте, хакеры могут атаковать организацию Вашего работодателя за счет уязвимостей, заложенных в системе мобильных устройств. Более того, группам реагирования на инциденты в области компьютерной безопасности может быть не под силу выявлять атаки, которые совершаются через мобильные устройства во время использования корпоративной электронной почты.

Как мы уже говорили, не все приложения, доступные в App Store и Google Play, являются полезными и безобидными, а в случае сторонних магазинов проблема носит еще более острый характер. Операторы магазинов прилагают немалые усилия, чтобы не дать вредоносным приложениям попасть на свои веб-сайты, однако некоторым подобным программам это все-таки удается. Такие приложения могут похищать важную информацию, пытаться выманить деньги или получить доступ к корпоративным сетям, к которым подключено устройство, показывать пользователям назойливую рекламу, а также выполнять ряд других грязных действий.

*Как удалить вредоносное ПО?*

Если Вы подозреваете, что на Вашем устройстве завелось вредоносное ПО, или просто хотите перестраховаться, пожалуйста, выполните несколько простых шагов.

Прежде всего, если Вы не сделали это раньше, загрузите проверенную [антивирусную программу](https://ru.malwarebytes.com/), например [Malwarebytes for Windows](https://ru.malwarebytes.com/premium/" \t "_blank), [Malwarebytes for Mac](https://ru.malwarebytes.com/mac/" \t "_blank), [Malwarebytes for Android](https://ru.malwarebytes.com/mobile/" \t "_blank) или [один из наших продуктов для бизнеса](https://ru.malwarebytes.com/business/). Затем установите программу и запустите проверку. Указанные программы выполняют поиск и устраняют все вредоносные объекты, обнаруженные на Вашем устройстве.

После того как система очищена от вирусов, рекомендуется сменить пароли – не только в учетной записи компьютера или мобильного устройства, но и в электронной почте, социальных сетях, часто посещаемых онлайн-магазинах, а также в банковских и биллинговых сервисах.

Если на Ваш iPhone каким-то образом проник враждебный объект, все оказывается несколько сложнее. Компания Apple не разрешает проверять ни системные файлы iPhone, ни другие файлы. В этом случае единственное решение – удалить все данные с телефона, выполнив сброс на заводские настройки, а затем восстановить файлы из резервной копии (которую Вы, разумеется, сделали раньше, верно?). Вы также можете попробовать установить защитные программы, блокирующие мошеннические звонки и текстовые сообщения, например Malwarebytes for iOS (скоро в продаже!).  
Если Вам нужна более подробная информация, пожалуйста, ознакомьтесь с заметкой Венди Заморы «[10 easy steps to clean your infected computer](https://blog.malwarebytes.com/101/2015/06/10-easy-steps-to-clean-your-infected-computer/)» (10 простых способов очистить зараженный компьютер).

*Как защититься от вредоносного ПО?*

Оставайтесь бдительны. Обращайте особое внимание на домены, которые представляют собой странную комбинацию букв и отличаются от привычных com, org, edu, biz и других, поскольку это может указывать на веб-сайт в группе риска.

«Всегда поддерживайте операционную систему, браузеры и плагины в актуальном состоянии».

На всех устройствах следите за возможным появлением ранних признаков заражения вредоносным ПО, чтобы не дать ему закрепиться в недрах системы.

Во время работы в сети Интернет не нажимайте на рекламные блоки во всплывающих окнах. Не открывайте вложения в электронных письмах, которые пришли от незнакомого отправителя, не загружайте программы с непроверенных веб-сайтов или через пиринговые сети.

Всегда поддерживайте операционную систему, браузеры и плагины в актуальном состоянии, поскольку своевременное получение обновлений поможет не подпускать киберпреступников слишком близко.

Пользователям мобильных устройств рекомендуется устанавливать приложения только из магазина Google Play (для пользователей iPhone единственным магазином является App Store). Всякий раз перед загрузкой нового приложения проверяйте его рейтинги и прилагаемые отзывы. Если рейтинги невысоки, а количество загрузок невелико, то такое приложение лучше не устанавливать.

Не загружайте приложения из сторонних источников. Мы рекомендуем вовсе отключить эту функцию в меню устройства Android. Для этого выберите пункт «Настройки» и перейдите к разделу «Безопасность». Затем отключите параметр «Неизвестные источники» – в этом случае Вы будете загружать приложения только из магазина Google Play.

Не нажимайте на странные непроверенные ссылки в электронных письмах, текстах и сообщениях WhatsApp, отправленных неизвестным отправителем. Следует также избегать странных ссылок, полученных от друзей или пользователей в списке контактов, – за исключением случаев, когда Вы убедились в их безопасности.

Стремясь защитить свой бизнес и избавить компьютерные сети от вредоносных приложений, организации могут применять строгие правила безопасного использования мобильных устройств, а также устанавливать средства защиты мобильных устройств для реализации этих правил. Это жизненно необходимо для современной корпоративной среды, в которой множество операционных систем совместно работают в различных зданиях.

Наконец, обзаведитесь надежной антивирусной программой. Она должна обладать многоуровневой защитой, позволяющей [проверять систему и обнаруживать вредоносное ПО](https://ru.malwarebytes.com/mwb-download/), например рекламное ПО и шпионские программы, а также в реальном времени проактивно блокировать другие угрозы, например атаки программ-вымогателей. Антивирусная программа также должна быть способна устранять последствия атак, восстанавливать ущерб, нанесенный вредоносным ПО, и возвращать системе нормальную функциональность.

Вместо того чтобы ожидать, когда вредоносное ПО нанесет удар по Вашему компьютеру, мобильному устройству или корпоративной сети, лучше ударить первым и загрузить [надежный антивирус, способный обеспечить Вашу кибербезопасность](https://ru.malwarebytes.com/), – [Malwarebytes for Windows](https://ru.malwarebytes.com/premium/" \t "_blank), [Malwarebytes for Mac](https://ru.malwarebytes.com/mac/" \t "_blank), [Malwarebytes for Android](https://ru.malwarebytes.com/mobile/" \t "_blank), [портативную версию продукта Malwarebytes](https://ru.malwarebytes.com/techbench/) или одно из [решений Malwarebytes для бизнеса.](https://ru.malwarebytes.com/business/) Ведь приятно осознавать, что Вы можете дать отпор компьютерному гриппу!

Создание, использование и распространение вредоносных программ относится к преступлениям, в сфере компьютерной информации, направленным против общественной безопасности и общественного порядка, ответственность за которые предусмотрена ст. 273 Уголовного кодекса РФ.

Уголовная ответственность наступает за создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств ее защиты.

Способом совершения данного преступления может быть только активное действие, которое выражено в виде создания, использования или распространения вредоносных компьютерных программ либо иной компьютерной информации.

Создание вредоносной программы - это результат деятельности, выразившейся в представлении в объективной форме совокупности данных и команд, предназначенных для нарушения нормального функционирования информационно-телекоммуникационных сетей и компьютерных устройств.

Использование компьютерных программ - это действия по введению таких программ или баз в хозяйственный оборот.

Распространение программ - это предоставление доступа к воспроизведению в любой материальной форме компьютерной программе, в том числе сетевыми и иными способами, а так же путем продажи, проката, сдачи внаем, предоставлением взаймы для любой из этих целей.

Данное преступление не требует наступления каких-либо последствий, уголовная ответственность возникает уже в результате создания, использования или распространения программы.

Уголовная ответственность за данное преступление наступает с 16 лет.

Максимальное наказание за вышеназванные деяния по данной статье предусмотрено в виде лишения свободы на срок до 7 лет если они повлекли тяжкие последствия или создали угрозу их наступления.

Создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации, -

наказываются ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо лишением свободы на тот же срок со штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев.

2. Деяния, предусмотренные [частью первой](http://www.consultant.ru/document/cons_doc_LAW_330816/a4d58c1af8677d94b4fc8987c71b131f10476a76/#dst981) настоящей статьи, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно причинившие [крупный ущерб](http://www.consultant.ru/document/cons_doc_LAW_330816/5c337673c261a026c476d578035ce68a0ae86da0/#dst979) или совершенные из корыстной заинтересованности, -

наказываются ограничением свободы на срок до четырех лет, либо принудительными работами на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового, либо лишением свободы на срок до пяти лет со штрафом в размере от ста тысяч до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от двух до трех лет или без такового и с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

3. Деяния, предусмотренные [частями первой](http://www.consultant.ru/document/cons_doc_LAW_330816/a4d58c1af8677d94b4fc8987c71b131f10476a76/#dst981) или [второй](http://www.consultant.ru/document/cons_doc_LAW_330816/a4d58c1af8677d94b4fc8987c71b131f10476a76/#dst983) настоящей статьи, если они повлекли тяжкие последствия или создали угрозу их наступления, -

наказываются лишением свободы на срок до семи лет.