**Профилактика заражения компьютерным вредоносным ПО**

**Правило № 1**: защитите компьютер с помощью антивирусных программ и программ безопасной работы в интернете. Для этого:

* Установите Антивирус.
* Регулярно обновляйте сигнатуры угроз, входящие в состав приложения. Обновление можно проводить раз в день при возникновении вирусных эпидемий .
* Установите рекомендуемые экспертами параметры для полной проверки компьютера и запланируйте ее выполнение не реже одного раза в неделю.

**Правило № 2**: будьте осторожны при записи новых данных на компьютер:

* Проверяйте на присутствие вирусов все съемные диски (дискеты, CD/DVD-диски, flash-карты и пр.) перед их использованием.
* Осторожно обращайтесь с почтовыми сообщениями. Не запускайте никаких файлов, пришедших по почте, если вы не уверены, что они действительно должны были прийти к вам.
* Внимательно относитесь к информации, получаемой из интернета. Если с какого-либо веб-сайта предлагается установить новую программу, обратите внимание на наличие у нее сертификата безопасности.
* Если вы копируете из интернета или локальной сети исполняемый файл, обязательно проверьте его с помощью Антивируса.
* Внимательно относитесь к выбору посещаемых интернет-ресурсов. Некоторые из сайтов заражены опасными скрипт-вирусами или интернет-червями.

**Правило № 3**: внимательно относитесь к информации от антивирусного ПО.

В большинстве случаев оно сообщает о начале новой эпидемии задолго до того, как она достигнет своего пика. Вероятность заражения в этом случае еще невелика, и, скачав обновленные сигнатуры угроз, защитите себя от нового вируса заблаговременно.

**Правило № 4**: пользуйтесь сервисом Windows Update и регулярно устанавливайте обновления операционной системы Microsoft Windows.

**Правило № 5**: покупайте лицензионные копии программного обеспечения у официальных продавцов.

**Правило № 6**: уменьшите риск неприятных последствий возможного заражения:

* Своевременно делайте резервное копирование данных. В случае потери данных система достаточно быстро может быть восстановлена при наличии резервных копий. Дистрибутивные диски, дискеты, флеш-карты и другие носители с программным обеспечением и ценной информацией должны храниться в надежном месте.

**Обзор антивирусных программ**

**Антивирусная программа (антивирус)**– специализированная [программа](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%BD%D0%BE%D0%B5_%D0%BE%D0%B1%D0%B5%D1%81%D0%BF%D0%B5%D1%87%D0%B5%D0%BD%D0%B8%D0%B5) для обнаружения компьютерных [вирусов](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D1%8B%D0%B9_%D0%B2%D0%B8%D1%80%D1%83%D1%81), а также нежелательных (считающихся [вредоносными](https://ru.wikipedia.org/wiki/%D0%92%D1%80%D0%B5%D0%B4%D0%BE%D0%BD%D0%BE%D1%81%D0%BD%D0%B0%D1%8F_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%B0)) программ и восстановления заражённых (модифицированных) такими программами [файлов](https://ru.wikipedia.org/wiki/%D0%A4%D0%B0%D0%B9%D0%BB) и профилактики – предотвращения заражения (модификации) файлов или [операционной системы](https://ru.wikipedia.org/wiki/%D0%9E%D0%BF%D0%B5%D1%80%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0) вредоносным кодом.

Существует большой выбор антивирусных программ, наиболее популярные:

* [ESET NOD32](https://infourok.ru/go.html?href=https%3A%2F%2Fwww.esetnod32.ru%2F)
* [Kaspersky](https://infourok.ru/go.html?href=http%3A%2F%2Fwww.kaspersky.ru)
* [Avast](https://infourok.ru/go.html?href=https%3A%2F%2Fwww.avast.ru%2F)
* [McAfee](https://infourok.ru/go.html?href=https%3A%2F%2Fwww.mcafee.com%2F)
* [Dr.Web](https://infourok.ru/go.html?href=https%3A%2F%2Fwww.drweb.ru%2F%3Flng%3Dru)
* [Avira](https://infourok.ru/go.html?href=https%3A%2F%2Fwww.avira.com%2F)
* [Comodo Antivirus](https://infourok.ru/go.html?href=https%3A%2F%2Fantivirus.comodo.com%2F)
* [Microsoft Security](https://infourok.ru/go.html?href=https%3A%2F%2Fwww.microsoft.com%2Fuk-ua%2Fdownload%2Fdetails.aspx%3Fid%3D5201)

Любая антивирусная программа имеет антивирусные базы, которые необходимо регулярно обновлять.

Антивирусная программа проверяет все открываемые, сохраняемые, запускаемые файлы, отслеживает подозрительные действия в компьютерной сети, сканирует жесткий диск и подключаемые внешние источники информации. При обнаружении вредоносных объектов антивирусная программа лечит зараженные объекты и помещает в карантин или удаляет вредоносное ПО, сообщая об этом пользователю. Рекомендуется периодически запускать полную проверку компьютера антивирусной программой.

**Профилактика заражения компьютерным вредоносным ПО**

**Правило № 1**: защитите компьютер с помощью антивирусных программ и программ безопасной работы в интернете. Для этого:

* Установите Антивирус.
* Регулярно обновляйте сигнатуры угроз, входящие в состав приложения. Обновление можно проводить раз в день при возникновении вирусных эпидемий .
* Установите рекомендуемые экспертами параметры для полной проверки компьютера и запланируйте ее выполнение не реже одного раза в неделю.

**Правило № 2**: будьте осторожны при записи новых данных на компьютер:

* Проверяйте на присутствие вирусов все съемные диски (дискеты, CD/DVD-диски, flash-карты и пр.) перед их использованием.
* Осторожно обращайтесь с почтовыми сообщениями. Не запускайте никаких файлов, пришедших по почте, если вы не уверены, что они действительно должны были прийти к вам.
* Внимательно относитесь к информации, получаемой из интернета. Если с какого-либо веб-сайта предлагается установить новую программу, обратите внимание на наличие у нее сертификата безопасности.
* Если вы копируете из интернета или локальной сети исполняемый файл, обязательно проверьте его с помощью Антивируса.
* Внимательно относитесь к выбору посещаемых интернет-ресурсов. Некоторые из сайтов заражены опасными скрипт-вирусами или интернет-червями.

**Правило № 3**: внимательно относитесь к информации от антивирусного ПО.

В большинстве случаев оно сообщает о начале новой эпидемии задолго до того, как она достигнет своего пика. Вероятность заражения в этом случае еще невелика, и, скачав обновленные сигнатуры угроз, защитите себя от нового вируса заблаговременно.

**Правило № 4**: пользуйтесь сервисом Windows Update и регулярно устанавливайте обновления операционной системы Microsoft Windows.

**Правило № 5**: покупайте лицензионные копии программного обеспечения у официальных продавцов.

**Правило № 6**: уменьшите риск неприятных последствий возможного заражения:

* Своевременно делайте резервное копирование данных. В случае потери данных система достаточно быстро может быть восстановлена при наличии резервных копий. Дистрибутивные диски, дискеты, флеш-карты и другие носители с программным обеспечением и ценной информацией должны храниться в надежном месте.

**Обзор антивирусных программ**

**Антивирусная программа (антивирус)**– специализированная [программа](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%BD%D0%BE%D0%B5_%D0%BE%D0%B1%D0%B5%D1%81%D0%BF%D0%B5%D1%87%D0%B5%D0%BD%D0%B8%D0%B5) для обнаружения компьютерных [вирусов](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D1%8B%D0%B9_%D0%B2%D0%B8%D1%80%D1%83%D1%81), а также нежелательных (считающихся [вредоносными](https://ru.wikipedia.org/wiki/%D0%92%D1%80%D0%B5%D0%B4%D0%BE%D0%BD%D0%BE%D1%81%D0%BD%D0%B0%D1%8F_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%B0)) программ и восстановления заражённых (модифицированных) такими программами [файлов](https://ru.wikipedia.org/wiki/%D0%A4%D0%B0%D0%B9%D0%BB) и профилактики – предотвращения заражения (модификации) файлов или [операционной системы](https://ru.wikipedia.org/wiki/%D0%9E%D0%BF%D0%B5%D1%80%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0) вредоносным кодом.

Существует большой выбор антивирусных программ, наиболее популярные:

* [ESET NOD32](https://infourok.ru/go.html?href=https%3A%2F%2Fwww.esetnod32.ru%2F)
* [Kaspersky](https://infourok.ru/go.html?href=http%3A%2F%2Fwww.kaspersky.ru)
* [Avast](https://infourok.ru/go.html?href=https%3A%2F%2Fwww.avast.ru%2F)
* [McAfee](https://infourok.ru/go.html?href=https%3A%2F%2Fwww.mcafee.com%2F)
* [Dr.Web](https://infourok.ru/go.html?href=https%3A%2F%2Fwww.drweb.ru%2F%3Flng%3Dru)
* [Avira](https://infourok.ru/go.html?href=https%3A%2F%2Fwww.avira.com%2F)
* [Comodo Antivirus](https://infourok.ru/go.html?href=https%3A%2F%2Fantivirus.comodo.com%2F)
* [Microsoft Security](https://infourok.ru/go.html?href=https%3A%2F%2Fwww.microsoft.com%2Fuk-ua%2Fdownload%2Fdetails.aspx%3Fid%3D5201)

Любая антивирусная программа имеет антивирусные базы, которые необходимо регулярно обновлять.

Антивирусная программа проверяет все открываемые, сохраняемые, запускаемые файлы, отслеживает подозрительные действия в компьютерной сети, сканирует жесткий диск и подключаемые внешние источники информации. При обнаружении вредоносных объектов антивирусная программа лечит зараженные объекты и помещает в карантин или удаляет вредоносное ПО, сообщая об этом пользователю. Рекомендуется периодически запускать полную проверку компьютера антивирусной программой.