**Билет 10**

Дать определение компьютерного вируса, их классификации. Признаки проявления компьютерных вирусов, их основные источники. Последствия действия компьютерных вирусов. Профилактика и лечение от компьютерных вирусов. Антивирусные программы, их классификация.

**Компьютерный вирус** — вид вредоносных программ, способных внедряться в код других программ, системные области памяти, загрузочные секторы и распространять свои копии по разнообразным каналам связи.

Основная цель вируса — его распространение. Кроме того, часто его сопутствующей функцией является нарушение работы программно-аппаратных комплексов — удаление файлов, удаление операционной системы, приведение в негодность структур размещения данных, нарушение работоспособности сетевых структур, кража личных данных, вымогательство, блокирование работы пользователей и т. п. Даже если автор вируса не запрограммировал вредоносных эффектов, вирус может приводить к сбоям компьютера из-за ошибок, неучтённых тонкостей взаимодействия с операционной системой и другими программами. Кроме того, вирусы, как правило, занимают место на накопителях информации и потребляют ресурсы системы.

**Компьютерный вирус** — вид [вредоносных программ](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), способных внедряться в [код](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%B4) других программ, системные области памяти, [загрузочные секторы](https://ru.wikipedia.org/wiki/%D0%97%D0%B0%D0%B3%D1%80%D1%83%D0%B7%D0%BE%D1%87%D0%BD%D1%8B%D0%B9_%D1%81%D0%B5%D0%BA%D1%82%D0%BE%D1%80) и распространять свои копии по разнообразным каналам связи.

Основная цель вируса — его распространение. Кроме того, часто его сопутствующей функцией является нарушение работы программно-аппаратных комплексов — удаление файлов, удаление операционной системы, приведение в негодность структур размещения данных, нарушение работоспособности сетевых структур, кража личных данных, вымогательство, блокирование работы пользователей и т. п. Даже если автор вируса не запрограммировал вредоносных эффектов, вирус может приводить к сбоям компьютера из-за ошибок, неучтённых тонкостей взаимодействия с [операционной системой](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) и другими программами. Кроме того, вирусы, как правило, занимают место на накопителях информации и потребляют ресурсы системы.

В обиходе «вирусами» называют всё вредоносное ПО, хотя на самом деле это лишь один его вид.

**Классификация**

Ныне существует немало разновидностей вирусов, различающихся по основному способу распространения и функциональности. Если изначально вирусы распространялись на [дискетах](https://ru.wikipedia.org/wiki/%D0%94%D0%B8%D1%81%D0%BA%D0%B5%D1%82%D0%B0) и [других носителях](https://ru.wikipedia.org/wiki/%D0%97%D0%B0%D0%BF%D0%BE%D0%BC%D0%B8%D0%BD%D0%B0%D1%8E%D1%89%D0%B5%D0%B5_%D1%83%D1%81%D1%82%D1%80%D0%BE%D0%B9%D1%81%D1%82%D0%B2%D0%BE), то сейчас доминируют вирусы, распространяющиеся через [локальные](https://ru.wikipedia.org/wiki/%D0%9B%D0%BE%D0%BA%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0%D1%8F_%D1%81%D0%B5%D1%82%D1%8C) и глобальные ([Интернет](https://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82)) сети. Растёт и функциональность вирусов, которую они перенимают от других видов программ.

В настоящее время не существует единой системы классификации и именования вирусов (хотя попытка создать стандарт была предпринята на встрече CARO в 1991 году). Принято разделять вирусы:

*По поражаемым объектам* ([файловые вирусы](https://ru.wikipedia.org/wiki/%D0%A4%D0%B0%D0%B9%D0%BB%D0%BE%D0%B2%D1%8B%D0%B9_%D0%B2%D0%B8%D1%80%D1%83%D1%81), [загрузочные вирусы](https://ru.wikipedia.org/wiki/%D0%97%D0%B0%D0%B3%D1%80%D1%83%D0%B7%D0%BE%D1%87%D0%BD%D1%8B%D0%B9_%D0%B2%D0%B8%D1%80%D1%83%D1%81), сценарные вирусы, [макровирусы](https://ru.wikipedia.org/wiki/%D0%9C%D0%B0%D0%BA%D1%80%D0%BE%D0%B2%D0%B8%D1%80%D1%83%D1%81%D1%8B), вирусы, поражающие исходный код). В свою очередь, файловые вирусы делят по механизму заражения: паразитирующие добавляют себя в исполняемый файл, перезаписывающие невосстановимо портят заражённый файл, «спутники» идут отдельным файлом.

*По поражаемым операционным системам и платформам* ([DOS](https://ru.wikipedia.org/wiki/DOS), [Windows](https://ru.wikipedia.org/wiki/Windows), [Unix](https://ru.wikipedia.org/wiki/Unix), [Linux](https://ru.wikipedia.org/wiki/Linux), [Android](https://ru.wikipedia.org/wiki/Android));

По используемым технологиям ([полиморфные вирусы](https://ru.wikipedia.org/wiki/%D0%9F%D0%BE%D0%BB%D0%B8%D0%BC%D0%BE%D1%80%D1%84%D0%BD%D1%8B%D0%B9_%D0%B2%D0%B8%D1%80%D1%83%D1%81), [стелс-вирусы](https://ru.wikipedia.org/wiki/%D0%A1%D1%82%D0%B5%D0%BB%D1%81-%D0%B2%D0%B8%D1%80%D1%83%D1%81), [руткиты](https://ru.wikipedia.org/wiki/%D0%A0%D1%83%D1%82%D0%BA%D0%B8%D1%82));

*По языку, на котором написан вирус* ([ассемблер](https://ru.wikipedia.org/wiki/%D0%AF%D0%B7%D1%8B%D0%BA_%D0%B0%D1%81%D1%81%D0%B5%D0%BC%D0%B1%D0%BB%D0%B5%D1%80%D0%B0), [высокоуровневый язык программирования](https://ru.wikipedia.org/wiki/%D0%92%D1%8B%D1%81%D0%BE%D0%BA%D0%BE%D1%83%D1%80%D0%BE%D0%B2%D0%BD%D0%B5%D0%B2%D1%8B%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D1%8F), [сценарный язык](https://ru.wikipedia.org/wiki/%D0%A1%D1%86%D0%B5%D0%BD%D0%B0%D1%80%D0%BD%D1%8B%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA) и др.);

*По дополнительной вредоносной функциональности* ([бэкдоры](https://ru.wikipedia.org/wiki/%D0%91%D1%8D%D0%BA%D0%B4%D0%BE%D1%80" \o "Бэкдор), [кейлоггеры](https://ru.wikipedia.org/wiki/%D0%9A%D0%B5%D0%B9%D0%BB%D0%BE%D0%B3%D0%B3%D0%B5%D1%80), [шпионы](https://ru.wikipedia.org/wiki/Spyware), [ботнеты](https://ru.wikipedia.org/wiki/%D0%91%D0%BE%D1%82%D0%BD%D0%B5%D1%82) и др.).

**Распространение**

Вирусы распространяются, копируя своё тело и обеспечивая его последующее исполнение: вписывая себя в исполняемый код других программ, заменяя собой другие программы, прописываясь в автозапуск через реестр и другое. Вирусом или его носителем могут быть не только программы, содержащие машинный код, но и любая информация, содержащая автоматически исполняемые команды, — например, пакетные файлы и документы Microsoft Word и Excel, содержащие макросы. Кроме того, для проникновения на компьютер вирус может использовать уязвимости в популярном программном обеспечении (например, Adobe Flash, Internet Explorer, Outlook), для чего распространители внедряют его в обычные данные (картинки, тексты и т. д.) вместе с эксплойтом, использующим уязвимость.

После того как вирус успешно внедрился в коды программы, файла или документа, он будет находиться в состоянии сна, пока обстоятельства не заставят компьютер или устройство выполнить его код. Чтобы вирус заразил ваш компьютер, необходимо запустить заражённую программу, которая, в свою очередь, приведёт к выполнению кода вируса. Это означает, что вирус может оставаться бездействующим на компьютере без каких-либо симптомов поражения. Однако, как только вирус начинает действовать, он может заражать другие файлы и компьютеры, находящиеся в одной сети. В зависимости от целей программиста-вирусописателя, вирусы либо причиняют незначительный вред, либо имеют разрушительный эффект, на пример удаление данных или кража конфиденциальной информации.

**Признаки проявления компьютерных вирусов**

* медленная работа компьютера;
* невозможность загрузки операционной системы;
* исчезновение файлов и каталогов или искажение их содержимого;
* изменение даты и времени модификации файлов;
* изменение размеров файлов;
* неожиданное значительное увеличение количества файлов на диске;
* существенное уменьшение размера свободной оперативной памяти;
* вывод на экран непредусмотренных сообщений или изображений;
* подача непредусмотренных звуковых сигналов;
* частые зависания и сбои в работе компьютера.

**Основные источники компьютерных вирусов**

[*Дискеты*](https://ru.wikipedia.org/wiki/%D0%94%D0%B8%D1%81%D0%BA%D0%B5%D1%82%D0%B0)*.* Самый распространённый канал заражения в 1980—1990-е годы. Сейчас практически отсутствует из-за появления более распространённых и эффективных каналов и отсутствия флоппи-дисководов на многих современных компьютерах.

[*Флэш-накопители*](https://ru.wikipedia.org/wiki/%D0%A4%D0%BB%D0%B5%D1%88-%D0%BF%D0%B0%D0%BC%D1%8F%D1%82%D1%8C) *(«флэшки»).* В настоящее время [USB-накопители](https://ru.wikipedia.org/wiki/USB_flash_drive) заменяют дискеты и повторяют их судьбу — большое количество вирусов распространяется через съёмные накопители, включая [цифровые фотоаппараты](https://ru.wikipedia.org/wiki/%D0%A6%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%BE%D0%B9_%D1%84%D0%BE%D1%82%D0%BE%D0%B0%D0%BF%D0%BF%D0%B0%D1%80%D0%B0%D1%82), цифровые видеокамеры, [портативные цифровые плееры](https://ru.wikipedia.org/wiki/%D0%A6%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%BE%D0%B9_%D0%BF%D1%80%D0%BE%D0%B8%D0%B3%D1%80%D1%8B%D0%B2%D0%B0%D1%82%D0%B5%D0%BB%D1%8C), а с 2000-х годов всё большую роль играют [мобильные телефоны](https://ru.wikipedia.org/wiki/%D0%A1%D0%BE%D1%82%D0%BE%D0%B2%D1%8B%D0%B9_%D1%82%D0%B5%D0%BB%D0%B5%D1%84%D0%BE%D0%BD), особенно [смартфоны](https://ru.wikipedia.org/wiki/%D0%A1%D0%BC%D0%B0%D1%80%D1%82%D1%84%D0%BE%D0%BD) (появились [мобильные вирусы](https://ru.wikipedia.org/wiki/%D0%9C%D0%BE%D0%B1%D0%B8%D0%BB%D1%8C%D0%BD%D1%8B%D0%B9_%D0%B2%D0%B8%D1%80%D1%83%D1%81)). Использование этого канала ранее было преимущественно обусловлено возможностью создания на накопителе специального файла [autorun.inf](https://ru.wikipedia.org/wiki/Autorun.inf), в котором можно указать программу, запускаемую [Проводником Windows](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D0%B2%D0%BE%D0%B4%D0%BD%D0%B8%D0%BA_Windows) при открытии такого накопителя. В [Windows 7](https://ru.wikipedia.org/wiki/Windows_7) возможность автозапуска файлов с переносных носителей была отключена.

[*Электронная почта*](https://ru.wikipedia.org/wiki/%D0%AD%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%BF%D0%BE%D1%87%D1%82%D0%B0)*.* Обычно вирусы в письмах электронной почты маскируются под безобидные вложения: картинки, документы, музыку, ссылки на сайты. В некоторых письмах могут содержаться действительно только ссылки, то есть в самих письмах может и не быть вредоносного кода, но если открыть такую ссылку, то можно попасть на специально созданный [веб-сайт](https://ru.wikipedia.org/wiki/%D0%92%D0%B5%D0%B1-%D1%81%D0%B0%D0%B9%D1%82), содержащий вирусный код. Многие почтовые вирусы, попав на компьютер пользователя, затем используют адресную книгу из установленных почтовых клиентов типа [Outlook](https://ru.wikipedia.org/wiki/Microsoft_Outlook) для рассылки самого себя дальше.

[*Системы обмена мгновенными сообщениями*](https://ru.wikipedia.org/wiki/Instant_messaging)*.* Здесь также распространена рассылка [ссылок](https://ru.wikipedia.org/wiki/%D0%93%D0%B8%D0%BF%D0%B5%D1%80%D1%81%D1%81%D1%8B%D0%BB%D0%BA%D0%B0) на якобы фото, музыку либо программы, в действительности являющиеся вирусами, по [ICQ](https://ru.wikipedia.org/wiki/ICQ) и через другие [программы мгновенного обмена сообщениями](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%B0_%D0%BC%D0%B3%D0%BD%D0%BE%D0%B2%D0%B5%D0%BD%D0%BD%D0%BE%D0%B3%D0%BE_%D0%BE%D0%B1%D0%BC%D0%B5%D0%BD%D0%B0_%D1%81%D0%BE%D0%BE%D0%B1%D1%89%D0%B5%D0%BD%D0%B8%D1%8F%D0%BC%D0%B8).

[*Веб-страницы*](https://ru.wikipedia.org/wiki/%D0%92%D0%B5%D0%B1-%D1%81%D1%82%D1%80%D0%B0%D0%BD%D0%B8%D1%86%D1%8B)*.* Возможно также заражение через страницы [Интернета](https://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82) ввиду наличия на страницах всемирной паутины различного «активного» содержимого: [скриптов](https://ru.wikipedia.org/wiki/%D0%A1%D0%BA%D1%80%D0%B8%D0%BF%D1%82), [ActiveX](https://ru.wikipedia.org/wiki/ActiveX)-компонент. В этом случае используются уязвимости [программного обеспечения](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), установленного на компьютере пользователя, либо уязвимости в ПО владельца сайта (что опаснее, так как заражению подвергаются добропорядочные сайты с большим потоком посетителей), а ничего не подозревающие пользователи, зайдя на такой сайт, рискуют заразить свой компьютер.

[*Интернет*](https://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82) *и* [*локальные сети*](https://ru.wikipedia.org/wiki/%D0%9B%D0%BE%D0%BA%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0%D1%8F_%D1%81%D0%B5%D1%82%D1%8C) *(*[*черви*](https://ru.wikipedia.org/wiki/%D0%A1%D0%B5%D1%82%D0%B5%D0%B2%D1%8B%D0%B5_%D1%87%D0%B5%D1%80%D0%B2%D0%B8)*).* Черви — вид вирусов, которые проникают на компьютер-жертву без участия пользователя. Черви используют так называемые «дыры» ([уязвимости](https://ru.wikipedia.org/wiki/%D0%A3%D1%8F%D0%B7%D0%B2%D0%B8%D0%BC%D0%BE%D1%81%D1%82%D1%8C_(%D0%BA%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%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))) в программном обеспечении операционных систем, чтобы проникнуть на компьютер. Уязвимости — это ошибки и недоработки в программном обеспечении, которые позволяют удалённо загрузить и выполнить машинный код, в результате чего вирус-червь попадает в операционную систему и, как правило, начинает действия по заражению других компьютеров через локальную сеть или Интернет. Злоумышленники используют заражённые компьютеры пользователей для рассылки [спама](https://ru.wikipedia.org/wiki/%D0%A1%D0%BF%D0%B0%D0%BC) или для [DDoS-атак](https://ru.wikipedia.org/wiki/DDoS-%D0%B0%D1%82%D0%B0%D0%BA%D0%B0).

**Последствия заражений компьютерными вирусами.**

### Если на компьютере заражено относительно мало программ, наличие вируса может быть практически незаметным. Однако по прошествии некоторого времени на компьютере мы видим последствия действия вирусов, на пример: некоторые программы перестают работать или начинают работать неправильно;

### компьютер начинает перезагрузку, либо не загружается вообще;

### на экран выводятся посторонние сообщения, символы и т.д.;

### работа на компьютере существенно замедляется;

### некоторые файлы удаляются, либо оказываются испорченными и т.д.

### повышенный расход трафика в интернете (несанкционированная рассылка электронных писем.

**Профилактика и лечение**

В настоящий момент существует множество антивирусных программ, используемых для предотвращения попадания вирусов в ПК. Однако нет гарантии, что они смогут справиться с новейшими разработками. Поэтому следует придерживаться некоторых мер предосторожности, в частности:

1. Не работать под привилегированными учётными записями без крайней необходимости (учётная запись администратора в Windows).
2. Не запускать незнакомые программы из сомнительных источников.
3. Стараться блокировать возможность несанкционированного изменения системных файлов.
4. Отключать потенциально опасную функциональность системы (например, autorun-носителей в MS Windows, сокрытие файлов, их расширений и пр.).
5. Не заходить на подозрительные сайты, обращать внимание на адрес в адресной строке обозревателя.
6. Пользоваться только доверенными дистрибутивами.
7. Постоянно делать резервные копии важных данных, желательно на носители, которые не стираются (например, BD-R) и иметь образ системы со всеми настройками для быстрого развёртывания.
8. Выполнять регулярные обновления часто используемых программ, особенно тех, которые обеспечивают безопасность системы.

### К этому моменту, как правило, уже достаточно много (или даже большинство) тех программ, с которыми вы работаете, являются зараженными вирусом, а некоторые файлы и диски — испорченными. Некоторые вирусы ведут себя очень коварно. Они вначале незаметно заражают большое число программ и дисков, а затем наносят очень серьезные повреждения, например, форматируют весь жесткий диск на компьютере, естественно после этого восстановить данные бывает просто невозможно. А бывают вирусы, которые ведут себя очень скрытно, и портят понемногу данные на жестком диске или сдвигают таблицу размещения файлов (FAT). К последним относится вирус OneHalf, имеющий множество модификаций.

### Таким образом, если не принимать мер по защите от вируса, то последствия заражения могут быть очень серьезными. Например, в начале 1989г. вирусом, написанным американским студентом Моррисом, были заражены и выведены из строя тысячи компьютеров, в том числе принадлежащих министерству обороны США. Автор вируса был приговорен судом к трем месяцам тюрьмы и штрафу в 270 тыс. дол. Наказание могло быть и более строгим, но суд учел, что вирус не портил данные, а только размножался. Для того, чтобы программа-вирус была незаметной, она должна иметь небольшие размеры. Поэтому вирусы пишут обычно на низкоуровневых языках Ассемблер или низкоуровневыми командами языка СИ.

**Классификации антивирусных программ**

Антивирусные программы подразделяются *по исполнению* (средствам блокирования) на:

* программные;
* программно-аппаратные.

*По признаку размещения в оперативной памяти* выделяют:

* резидентные (начинают свою работу при запуске операционной системы, постоянно находятся в памяти компьютера и осуществляют автоматическую проверку файлов);
* нерезидентные (запускаются по требованию пользователя или в соответствии с заданным для них расписанием).

*По виду (способу) защиты от вирусов различают*:

* Программы-детекторы, или сканеры, находят вирусы в оперативной памяти, на внутренних и(или) внешних носителях, выводя сообщение при обнаружении вируса.
* Программы-доктора, (фаги, полифаги) находят зараженные файлы и «лечат» их. Среди этого вида программ существуют полифаги, которые способны удалять разнообразные виды вирусов, самые известные из антивирусов-полифагов Norton AntiVirus, Doctor Web, Kaspersky Antivirus.
* Программы-вакцины (иммунизаторы) выполняют иммунизацию системы (файлов, каталогов) блокируя действие вирусов.
* Программы-ревизоры являются наиболее надежными в плане защиты от вирусов. Ревизоры запоминают исходное состояние программ, каталогов, системных областей диска до момента инфицирования компьютера (как правило, на основе подсчета контрольных сумм), затем сравнивают текущее состояние с первоначальным, выводя найденные изменения на дисплей.
* Программы-мониторы начинают свою работу при запуске операционной системы, постоянно находятся в памяти компьютера и осуществляют автоматическую проверку файлов по принципу «здесь и сейчас».
* Программы-фильтры (сторожа) обнаруживают вирус на ранней стадии, пока он не начал размножаться. Программы-сторожа — небольшие резидентные программы, целью которых является обнаружение действий, характерных для вирусов.