

Компьютерные вирусы и антивирусные программы

Вредоносные программы портят данные и воруют сведения, а антивирус помогает их обнаружить и остановить.



Почему эта тема важна для школьника

С угрозами чаще всего сталкиваются при скачивании игр и программ, переходе по подозрительным ссылкам, открытии вложений и использовании чужих флешек. Важно понимать, как защищать файлы, пароли и личные данные.



Что такое компьютерный вирус

Компьютерный вирус — это вредоносная программа, которая внедряется в файл или в систему и запускается без согласия пользователя. Часто он копируется и продолжает заражать устройство.

Вирус может менять работу других программ: удалять или повреждать данные, нарушать настройки и вызывать ошибки. Из-за этого страдают документы, фото и учебные материалы.

Важная особенность: вирус не «случайная» ошибка. Его цель — причинять вред или скрытно действовать на компьютере, а затем передаваться дальше через заражённые файлы и носители.

Как вирус попадает на устройство

Скачивания, вложения и поддельные загрузки

Заражение начинается, когда скачивают файлы из ненадёжных источников, открывают вложения в письмах и устанавливают поддельные игры или программы. Иногда пользователь нажимает на фальшивые кнопки «Скачать» и запускает заражённый файл.

Опасные файлы и запуск через макросы

Вирусы часто распространяются через файлы с расширениями .exe, .zip и .rar, а также через документы с опасными макросами. Запуская такой файл, человек запускает цепочку: ссылка или документ → запуск → заражение компьютера.

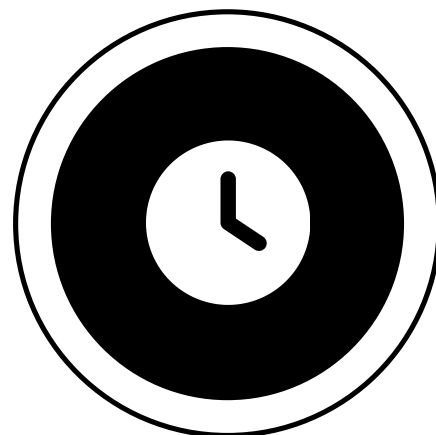
Главные источники заражения

Во многих случаях риск появляется после действий пользователя: при запуске неизвестного файла или переходе по ссылке, которая выглядит «как обычно».

Диаграмма показывает: угрозы чаще возникают не из «ниоткуда», а после неосторожных кликов и установок. Значит, профилактика начинается с привычек.

Учебный пример для наглядности, без привязки к конкретной статистике (обновлено:

Признаки заражения компьютера



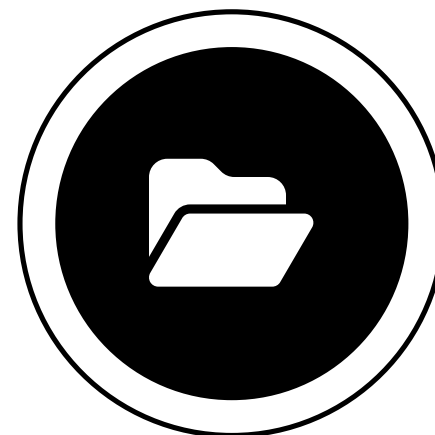
Замедление работы

Компьютер дольше запускает программы, приложения открываются «с задержкой». В фоне могут идти лишние процессы, поэтому устройство начинает работать заметно медленнее.



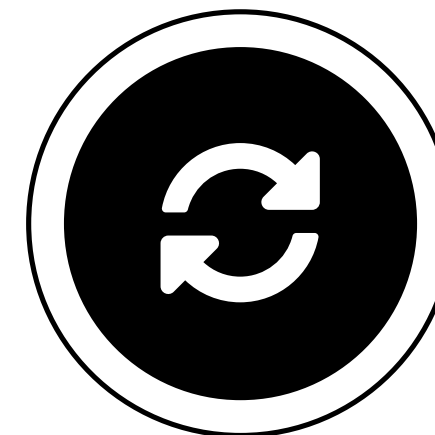
Всплывающая реклама и странные окна

Появляются навязчивые баннеры, может изменяться стартовая страница браузера. Иногда реклама всплывает даже там, где раньше её не было.



Исчезновение или повреждение файлов

Документы могут пропадать, а папки — неожиданно менять содержимое. Иногда файлы открываются с ошибкой или становятся недоступными после перезагрузки.



Самопроизвольные перезагрузки

Система может перезапускаться без предупреждения или «зависать» перед перезапуском. Такое поведение часто связано с вредоносными действиями в настройках.

Основные виды вредоносных программ

Таблица помогает различать тип угрозы по способу действия и характерному ущербу.

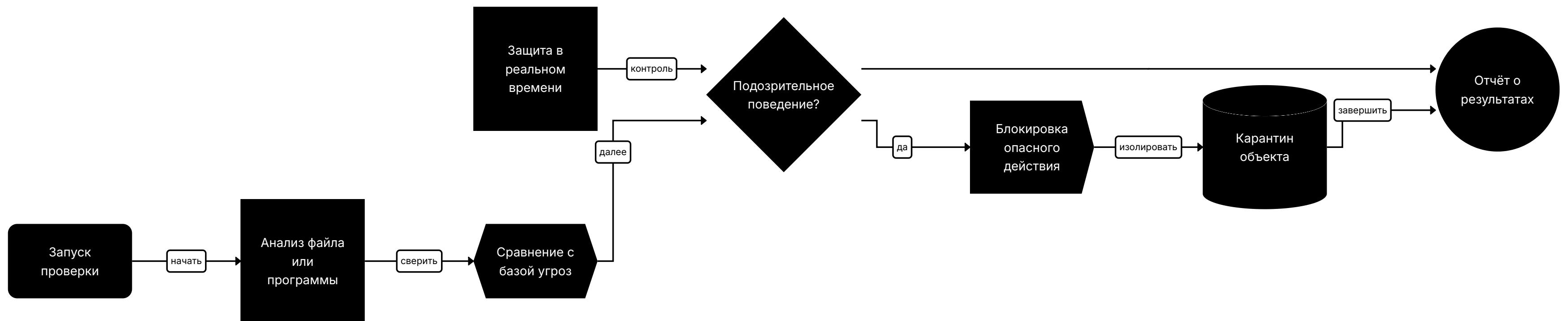
Разные виды вреда отличаются по цели: одни распространяются, другие крадут данные, а шифровальщики «останавливают» работу с файлами.

Вид	Способ действия	Главный вред
Вирус	Внедряется в файлы	Распространяет заражение
Троян	Маскируется под полезное	Устраивает скрытые действия
Червь	Быстро копируется по сети	Расширяет заражение
Шпионская программа	Собирает данные	Утечка информации
Шифровальщик	Блокирует доступ к файлам	Требует выкуп

Обобщение учебных классификаций по типам вредоносного ПО (без привязки к конкретной статистике).

Как антивирус обнаруживает угрозы

Пошаговая логика проверки: от анализа файлов до решения о блокировке или карантине.



Что умеет антивирусная программа

Антивирус ищет известные угрозы по сигнатурам — это характерные «отпечатки» вредоносных файлов. Поэтому важны обновления: новые угрозы появляются постоянно.

Он анализирует поведение программ и предупреждает об опасных сайтах. Если загрузка выглядит подозрительно, антивирус старается остановить её или сообщить о риске пользователю.

Многие антивирусы умеют сканировать флешки и внешние диски. Это полезно в школе, когда устройства подключают к разным компьютерам и возможен перенос заражённых файлов.

Этапы обнаружения угроз

Различайте быстрые проверки отдельных файлов и полную проверку устройства: вторая дольше, но обычно охватывает больше областей системы.

На эффективность влияет не только алгоритм поиска, но и актуальные данные. Обновление баз делает сигнатуры и правила распознавания точнее.

Схема основана на типовом пользовательском сценарии работы антивируса (обновлено: 2026-05).

Карантин, лечение и удаление файлов

01

Карантин изолирует подозрительный файл, чтобы он не запускался и не наносил вред системе. Антивирус проверяет объект и, если это возможно, предлагает безопасное решение до появления последствий.

02

Если антивирус умеет «вылечить» файл, он удаляет вредную часть и пытается восстановить исходное содержимое. Когда восстановление не получается, объект удаляется, либо остается только в карантине.

Почему антивирус не дает полной гарантии

Вредоносные программы постоянно меняются: авторы обновляют код, добавляют новые методы маскировки и обхода проверок. Из-за этого антивирус может не сразу распознать появившуюся «новинку».

Некоторые угрозы ведут себя тихо и «ждут» подходящего момента до запуска, поэтому признаки появляются не сразу. Другие используют современные способы, которые осложняют обнаружение по старым правилам.

Даже лучший антивирус зависит от актуальности баз и алгоритмов. Без обновлений системы и защитных модулей уязвимости остаются открытыми, и вредоносному коду проще получить доступ к данным.

Поэтому защита строится вместе: аккуратность при загрузке файлов и ссылок снижает риск заражения, а резервные копии помогают вернуть документы, если атака все же произошла.

Способы защиты и их роль

► Таблица показывает, что делает каждый способ защиты и как быстро он помогает в ситуации, когда возникает подозрение на угрозу.

► Антивирус и обновления уменьшают риск «прямого попадания», пароли защищают доступ к аккаунтам, а резервные копии и осторожность работают как страховка при ошибках пользователя.

Антивирус	Обновления системы	Сложные пароли	Резервные копии	Осторожность в интернете
Находит и блокирует угрозы	Закрывает уязвимости	Защищает учетные записи	Помогает восстановить файлы	Снижает вероятность заражения
При обнаружении — быстро	Постоянно снижает риск	Действует каждый вход	После инцидента	Каждый раз при действии

Обобщение функций защитных мер из школьного курса ИТ-безопасности; без привязки к конкретным продуктам.

Правила безопасного поведения в сети

01

Проверяй сайт перед входом

Смотри на адрес сайта и наличие признаков подлинности. Не вводи пароль и личные данные на незнакомых страницах, даже если оформление выглядит похоже на известные сервисы.

02

Скачивай только из официальных источников

Игры и программы ставь с сайтов разработчиков или из доверенных магазинов приложений. Пиратские версии часто содержат скрытый вредоносный код и вредят устройству.

03

Не открывай подозрительные окна и вложения

Если всплывает странное сообщение или предлагается «срочно что-то установить», закрой окно. Осторожно относись к письмам и вложениям: документы могут запускать опасные макросы.

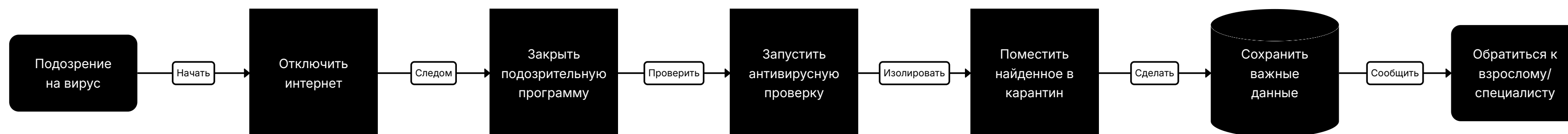
04

Проверяй любые «подарки» и странные запросы

Не переходи по ссылкам с обещаниями призов, скидок или бесплатных игр. Если появляется необычный запрос, сначала посоветуйся со взрослым или учителем.

Что делать при подозрении на вирус

Пошаговый алгоритм действий, чтобы снизить риск повреждения данных и распространения угрозы.



Какие функции антивируса важнее всего

На практике ключевое — постоянный контроль и актуальность защитных баз. Остальные модули усиливают безопасность, но без своевременных обновлений риск остается.

Диаграмма показывает: в центре защиты — непрерывная работа и обновления, а затем изоляция угроз и контроль веб-активности. Проверка флешек важна, потому что заражение часто начинается с внешних носителей.

Общая логика работы защитных модулей; значения даны по условной шкале для визуального сравнения.

Краткая история антивирусов

Конец 1980-х

Первые антивирусные программы появились, когда вредоносные файлы активно распространялись через дискеты и ранние сети. Тогда внимание уделяли обнаружению знакомых типов угроз по заметным признакам.

Переход к базам сигнатур

Со временем основным инструментом стали сигнатуры — «отпечатки» известных вредоносных программ. Антивирусы учились распознавать угрозы по характерным особенностям файлов.

Облачные базы и анализ поведения

Далее добавились облачные базы и поведенческий анализ. Защита стала учитывать не только содержимое, но и то, что программа делает после запуска.

Современный многоуровневый подход

Современные решения работают быстрее и комбинируют разные методы: от обновляемых баз до фильтров для веб-активности. Благодаря этому они могут реагировать и на подозрительные действия.

Как выбрать антивирус для дома и школы



Мифы о вирусах и защите



«Вирусы бывают только на компьютере»

Иногда кажется, что угрозы существуют лишь для ПК, но вредоносные программы встречаются и на смартфонах, и на планшетах. Заражение может начинаться с привычного на вид приложения, ссылки или даже уведомления.

Поэтому безопасность нужна на всех устройствах и во всех приложениях, где ты вводишь данные.



«Один антивирус решает всё»

Некоторые думают, что достаточно установить антивирус, и можно не соблюдать осторожность. На деле вредоносные файлы меняются, а заражение часто стартует с обычного файла или обманной ссылки. Без обновлений системы, резервных копий и внимательности к скачиваниям защита будет неполной.

Главная идея: безопасность — это привычка + защита

Компьютерные вирусы вредят файлам, паролям и нормальной работе устройства, а антивирус помогает находить и блокировать многие угрозы. Полная защита держится на комплексе мер и внимательном поведении в интернете.