МОСКОВСКИЙ АВИАЦИОННЫЙ ИНСТИТУТ

(НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ)

Факультет компьютерных наук и прикладной математики

Кафедра вычислительной математики и программирования

**Реферат**

**по курсу**

**«Вычислительные системы»**

«Компьютерные вирусы»

**Выполнил:**

студент группы М8О-108Б-22

Формалёв Александр Сергеевич

**Преподаватель:**

Сахарин Никита Александрович

Дата:

Подпись:

Москва, 2022

Оглавление

[Введение 3](#_Toc124184151)

[Определение компьютерного вируса и первое появление 4](#_Toc124184152)

[Способы распространения вирусов 6](#_Toc124184153)

[Классификация вирусов 9](#_Toc124184154)

[Способы противодействия компьютерным вирусам 12](#_Toc124184155)

[Заключение 13](#_Toc124184156)

[Источники 14](#_Toc124184157)

# Введение

В настоящее время компьютеры являются неотъемлемой частью жизни практически каждого человека. С помощью них люди открыли для себя новые возможности и даже новую науку. Стало возможным читать на компьютере, смотреть фильмы, играть в игры, производить вычисления, на которые у человека ушла бы вся жизнь, и многое другое. Никто и не мог подумать, что у этой «волшебной» машины могут быть болезни, наличие которых свойственно живому существу. Но в итоге появились так называемые компьютерные вирусы, из-за которых компьютер не мог полноценно функционировать. О том, что это такое и как с этим бороться, я расскажу далее.

# Определение компьютерного вируса и первое появление

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

Основной целью каждого вируса является его распространение, а сопутствующей функцией – нарушение работы программно-аппаратных комплексов (удаление файлов, удаление ОС, кража личных данных и т.д.).

Идея компьютерных вирусов впервые обсуждалась в серии лекций Джона фон Неймана в конце 1940-х годов, а уже в 1966 году вышла его монография «Теория самовоспроизводящихся автоматов». По сути, это мысленный эксперимент, рассматривающий возможность существования «механического» организма, например, компьютерного кода, который бы повреждал машины, создавал собственные копии и заражал новые машины подобно биологическому вирусу.

Первыми известными вирусами являются Virus 1, 2, 3 и Elk Cloner, появившиеся в 1981 году. Интересен был Elk Cloner тем, что он был обнаружен на компьютерах пользователей, а не в системе, в которой он был разработан. Вирус был написан пятнадцатилетним школьником Ричардом Скрента. Программа не влияла на работу компьютера и могла лишь случайно повредить диски. Вирус распространялся через дискеты: когда компьютер загружался с заражённой дискеты, запускалась копия вируса, а когда происходил доступ к незаражённой дискете, вирус копировал себя уже туда и т.д. Спустя три года после создания первых вирусов появились и первые антивирусные утилиты, способные бороться с вредоносными программами.

Далее стали появляться новые вирусы и даже вирусные эпидемии. Первым таким случаем можно назвать события, происходящие в 1987 году. Именно тогда был обнаружен вирус Brain, который заразил только в США более 18 тысяч компьютеров. Саму программу написали 2 брата из Пакистана, Базист и Амжад Фарук Альви в целях отслеживания пиратских копий их медицинского программного обеспечения, но не для нанесения какого-то вреда. Заражение вирусом происходило путём записи копии вируса в загрузочный сектор дискеты. Старая информация переносилась в другой сектор и помечалась как повреждённая. Вирус замедлял работу дискеты и делал 7 килобайт памяти недоступными для операционной системы. Также он стал первым стелс-вирусом, т.к. в Brain была встроена проверка, которая не позволяла ему заражать жёсткий диск, потому что программа не была предназначена для работы с ним. Именно поэтому вирус часто оставался незамеченным, особенно, когда пользователь не обращал внимания на замедление работы дискет.

Важным событием в истории развития вирусов стало создание в 1988 году Робертом Моррисом-младшим первого массового сетевого червя. Вирус имел целью скрытно проникнуть в вычислительные системы и остаться там необнаруженным. Программа могла раскрывать пароли, что позволяло программе маскироваться под задачу легальных пользователей системы. При сканировании [компьютера](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80) червь определял, инфицирован ли уже компьютер или нет, и [случайным образом](https://ru.wikipedia.org/wiki/%D0%93%D0%B5%D0%BD%D0%B5%D1%80%D0%B0%D1%82%D0%BE%D1%80_%D0%BF%D1%81%D0%B5%D0%B2%D0%B4%D0%BE%D1%81%D0%BB%D1%83%D1%87%D0%B0%D0%B9%D0%BD%D1%8B%D1%85_%D1%87%D0%B8%D1%81%D0%B5%D0%BB" \o "Генератор псевдослучайных чисел) выбирал, перезаписывать ли существующую копию, дабы обезопаситься от уловки с поддельной копией, внесённой [системными администраторами](https://ru.wikipedia.org/wiki/%D0%A1%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%BD%D1%8B%D0%B9_%D0%B0%D0%B4%D0%BC%D0%B8%D0%BD%D0%B8%D1%81%D1%82%D1%80%D0%B0%D1%82%D0%BE%D1%80" \o "Системный администратор). С определённой периодичностью программа, так или иначе, перезаписывала свою копию. Слишком маленькое число, заданное Робертом для описания периодичности, и послужило причиной первой в мире эпидемии сетевого червя. В итоге из-за незначительной ошибки создателя компьютеры многократно заражались червём, а каждый дополнительный экземпляр замедлял работу компьютера до состояния отказа от обслуживания. Также червь использовал маскировку: он удалял свой исполняемый файл, переименовывал свой процесс в sh и каждые три минуты ветвился. Ущерб от червя был оценён примерно в 96,5 миллионов долларов. Примерное число поражённых интернет-узлов – 6000.

Далее в 1989 году появился новый вирус DATACRIME, который заразил огромное количество компьютеров. Начиная с 13 октября и до конца каждого года вирус стирал данные с компьютеров, остальное время он просто распространялся. Вирус сканировал диск, заражая файлы с расширением [.COM](https://ru.wikipedia.org/wiki/.COM), пытаясь при этом избежать заражения файла COMMAND.COM. Далее вирус форматировал первые 9 дорожек жёсткого диска и выводит на экран сообщение: DATACRIME VIRUS RELEASED: 1 MARCH 1989. У вируса было несколько вариаций. Самая первая, Datacrime.1280, отличалась от оригинального вируса всего на несколько байтов. Версия Datacrime.II научилась заражать файлы с расширением [.EXE](https://ru.wikipedia.org/wiki/.EXE), сменила выводящийся текст на «DATACRIME II VIRUS», а код вируса был практически полностью зашифрован. Баги в прошлых версиях вируса были исправлены. Версия Datacrime.II.B была уже полностью зашифрована.

В том же году появилась первая в мире троянская программа AIDS. Вирус прикрывался под видом электронного письма с пояснениями о том, как избежать заражения СПИДом. AIDS способен перезаписывать .COM файлы и нарушать работу системы. Интереснее стала вариация вируса AIDS II. Этот вирус использовал функцию операционной системы, которая заключалась в том, что когда файл существует как в форме COM, так и в форме EXE, то выполняется форма COM. Т.о. вирус сначала находил незаражённый EXE файл, затем заражал его и создавал COM файл с вирусным кодом. На экран выводилось какое-либо послание, в том числе с вымоганием денег, а компьютер становился недоступным к работе.

# Способы распространения вирусов

В свое время наибольшую распространенность имели именно классические вирусы - но их создатели редко задавались конкретной целью навредить конечному пользователю, а скорее создавались из познавательных целей. Нынешние же вирусописатели преследуют абсолютно четкие и понятные цели – деньги, и их "детища" стали куда опаснее своих предшественников.

Самые опасные хищники сегодняшнего информационного пространства – это Трояны и Черви. Троян или troj получил свое название благодаря сходству между методом заражения и знаменитым тактическим ходом при осаде Трои. Пример заражения трояном – вам приходит письмо с текстом вложенными файлами с расширением ".JPG". Вот эти самые файлы это и есть троянский конь в недрах которого спрятан вредоносный код. Наиболее часто встречающиеся источники заражения - электронная почта, сайты знакомств, сайты с музыкой, сайты с бесплатным ПО. Что делает "троян"? Как правило, его задача открыть путь для остальных вирусов, выступить первым плацдармом.

Червь или Worm-. Особенность этих программ в эволюции и автономности. Червь попадая на компьютер как правило атакует почтовые программы и интернет пейджеры. После получения доступа к почте или пейджеру он начинает рассылать письма/сообщения содержащие видоизмененную версию самого себя. После чего либо самоликвидируется, либо заражает запускаемые файлы (EXE, COM, BAT). Поскольку вирус самоизменяется то до момента определения его в базе вашего антивируса он неуязвим.

Вирус находит и "заражает" другие программы, а также выполняет какие-нибудь вредные действия (например, портит файлы или таблицу размещения файлов (FAT) на диске, "засоряет" оперативную память и т.д.). Для маскировки вируса действия по заражению других программ и нанесению вреда могут выполняться не всегда, а скажем, при выполнении определенных условий. После того как вирус выполнит нужные ему действия, он передает управление той программе, в которой он находится, и она работает как обычно. Тем самым внешне работа зараженной программы выглядит так же, как и незараженной. Многие разновидности вирусов устроены так, что при запуске зараженной программы вирус остается в памяти компьютера и время от времени заражает программы и выполняет нежелательные действия на компьютере. Все действия вируса могут выполняться очень быстро и без выдачи каких либо сообщений, по этому пользователю очень трудно, практически невозможно, определить, что в компьютере происходит что-то необычное. Пока на компьютере заражено относительно мало программ, наличие вируса может быть практически незаметным. Однако по прошествии некоторого времени на компьютере начинает твориться что-то странное, например:  
- некоторые программы перестают работать или начинают работать неправильно

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

- работа на компьютере существенно замедляется

- некоторые файлы оказываются испорченными и т.д.

К этому моменту, как правило, уже достаточно много (или даже большинство) техпрограмм, с которыми вы работаете, являются зараженными вирусом, а некоторые файлы и диски — испорченными. Более того, зараженные программы с Вашего компьютера могли быть уже перенесены с помощью дискет или локальной сети на компьютеры ваших коллег и друзей. 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). Таким образом, если не принимать мер по защите от вируса, то последствия заражения могут быть очень серьезными.

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. Вирусы пишутся опытными программистами, или студентами просто из любопытства, или для отместки кому-либо или предприятию, которое обошлось с ними недостойным образом, или в коммерческих целях, или в целях направленного вредительства. Какие бы цели не преследовал автор, вирус может оказаться на вашем компьютере и постарается произвести те же вредные действия, что и у того, для кого он был создан. Следует заметить, что написание вируса — не такая уж сложная задача, вполне доступная изучающему программирование студенту. Поэтому еженедельно в мире появляются все новые и новые вирусы. И многие из них сделаны в нашей стране.

Некоторые виды файлов вирус может "заразить". Это означает, что вирус может "внедриться" в эти файлы, т.е. изменить их так, что они будут содержать вирус, который при некоторых обстоятельствах может начать свою работу. Следует заметить, что тексты программ и документов, информационные файлы баз данных, таблицы табличных процессоров и другие аналогичные файлы не могут быть заражены обычным вирусом, он может их только испортить. Заражение подобных файлов делается только Макро-вирусами. Эти вирусы могут заразить даже ваши документы Загрузчик операционной системы и главная загрузочная запись жесткого диска. Вирусы, поражающие эти области, называются загрузочными или BOOT-вирусами. Такой вирус начинает свою работу при начальной загрузке компьютера и становится резидентными, т.е. постоянно находится в памяти компьютера. Механизм распространения – заражение загрузочных записей вставляемых в компьютер дискет. Часто такие вирусы состоят из двух частей, поскольку загрузочная запись имеет небольшие размеры и в них трудно разместить целиком программу вируса. Часть вируса располагается в другом участке диска, например в конце корневого каталога диска или в кластере в области данных диска (обычно такой кластер объявляется дефектным, чтобы исключить затирание вируса при записи данных).

Драйверы устройств Файлы, указываемые в предложении DEVICE файла CONFIG.SYS. Вирус, находящийся в них начинает свою работу при каждом обращении к соответствующему устройству. Вирусы, заражающие драйверы устройств, очень мало распространены, поскольку драйверы редко переписывают с одного компьютера на другой. То же относится и к системным файлам DOS (MSDOS.SYS и IO.SYS) – их заражение также теоретически возможно, но для распространения вируса малоэффективно Как правило, каждая конкретная разновидность вируса может заражать только один или два типа файлов. Чаще всего встречаются вирусы, заражающие исполняемые файлы. На втором месте по распространенности загрузочные вирусы. Некоторые вирусы заражают и файлы, и загрузочные области дисков. Вирусы, заражающие драйверы устройств, встречаются крайне редко, обычно такие вирусы умеют заражать и исполняемые файлы.

# Классификация вирусов

Вирусы можно разделить на классы по следующим признакам:

**1. По среде обитания:**

Их подразделяют на файловые, загрузочные и файлово-загрузочные.

Файловым называют вирус, который внедряется в исполняемые файлы. Это означает, что код программы-вируса находится в каком-то исполняемом файле. Файл, в теле которого присутствует код программы-вируса, называется зараженным (инфицированным) файлом.

Загрузочным (бутовым) называют вирус, который внедpяется  в  загpузочный    сектоp    диска (Boot-сектоp), либо в сектоp, содеpжащий системный  загpузчик  винчестеpа (Master Boot Record). В данном случае код программы-вируса (или его часть) размещен в загрузочном секторе или в главной загрузочной записи. Диск, загрузочный сектор которого поражен вирусом, называется зараженным или инфицированным диском.

Файлово-загрузочным называют виpус, который внедряется как в файлы, так и загpузочные сектоpы дисков. Это уже более сложные вирусы, потому что они реализовывают и алгоpитм заражения файловым вирусом, и алгоритм заражения загрузочным вирусом.

**2. По способу заражения:**

Различают резидентные и нерезидентные.

Резидентный виpус размещает себя или некоторую свою часть в опеpативной памяти компьютера, получая возможность пеpехватывать обpащения опеpационной  системы  к  дискам и файлам. При обращении операционной системы к этим объектам, вирус внедряется в них. Резидентный виpус находится в опеpативной памяти и является активным (т.е. способным заражать все новые и новые объекты) вплоть до выключения или перезагрузки компьютеpа. Резидентными являются все загрузочные вирусы.

Нерезидентный виpус не заpажает оперативную память  компьютеpа, то есть не размещает свой код в оперативной памяти. Он является активным только во время работы зараженной программы.

**3. По деструктивным возможностям:**

Выделяют опасные и неопасные.

Неопасные виpусы - это те, которые либо совсем никак  не  влияют на  pаботу  компьютеpа,  кpоме того, что все-таки уменьшают свободную память на диске в pезультате своего pаспpостpанения, либо ограничиваются видео и аудиоэффектами.

Опасными виpусами являются все остальные. Это вирусы, котоpые наносят любой вред компьютеру: пpиводят к  сеpьезным сбоям в pаботе, уничтожают или изменяют данные, уничтожают информацию в системных областях компьютера и т.п.

**4. По особенностям алгоритма функционирования:**

Вирусы делят на изменяющие и не изменяющие среду обитания при распространении.

**Вирусы, не изменяющие среду обитания, делятся на 2 группы: вирусы-спутники и вирусы-черви.**

Вирусы-спутники не изменяют файлы. Механизм их действия состоит в создании копий исполняемых файлов. Например, в MS-DOS такие вирусы создают копии для файлов, имеющих расширение .ЕХЕ. Копии присваивается то же имя, что и исполняемому файлу, но расширение изменяется на .СОМ. При запуске файла с общим именем операционная система первым загружает на выполнение файл с расширением .СОМ, который является программой-вирусом. Файл-вирус запускает затем и файл с расширением .ЕХЕ.

Вирусы-черви попадают в рабочую станцию из сети, вычисляют адреса рассылки вируса по другим абонентам сети и осуществляют передачу вируса. Вирус не изменяет файлов и не записывается в загрузочные секторы дисков. Некоторые вирусы-черви создают рабочие копии вируса на диске, другие - размещаются только в оперативной памяти ЭВМ.

**Вирусы, изменяющие среду обитания, делятся на 2 группы: стелс-вирусы и полиморфные вирусы.**

Стелс-вирусы маскируют свое присутствие в среде обитания путем перехвата обращений операционной системы к пораженным файлам, секторам и переадресуют ОС к незараженным участкам информации. Вирус является резидентным, маскируется под программы ОС, может перемещаться в памяти. Такие вирусы активизируются при возникновении прерываний, выполняют определенные действия, в том числе и по маскировке, и только затем управление передается на программы ОС, обрабатывающие эти прерывания. Стелс-вирусы обладают способностью противодействовать резидентным антивирусным средствам.

Полиморфные вирусы не имеют постоянных опознавательных групп - сигнатур. Обычные вирусы для распознавания факта заражения среды обитания размещают в зараженном объекте специальную опознавательную двоичную последовательность или последовательность символов (сигнатуру), которая однозначно идентифицирует зараженность файла или сектора. Сигнатуры используются на этапе распространения вирусов для того, чтобы избежать многократного заражения одних и тех же объектов, так как при многократном заражении объекта значительно возрастает вероятность обнаружения вируса. Для устранения демаскирующих признаков полиморфные вирусы используют шифрование тела вируса и модификацию программы шифрования. За счет такого преобразования полиморфные вирусы не имеют совпадений кодов.

# Способы противодействия компьютерным вирусам

Способы противодействия компьютерным вирусам можно разделить на несколько групп: профилактика вирусного заражения и уменьшение предполагаемого ущерба от такого заражения; методика использования антивирусных программ, в том числе обезвреживание и удаление известного вируса; способы обнаружения и удаления неизвестного вируса.

Наиболее эффективны в борьбе с компьютерными вирусами антивирусные программы. Однако сразу хотелось бы отметить, что не существует антивирусов, гарантирующих стопроцентную защиту от вирусов, и заявления о существовании таких систем можно расценить как либо недобросовестную рекламу, либо непрофессионализм. Таких систем не существует, поскольку на любой алгоритм антивируса всегда можно предложить контр-алгоритм вируса, невидимого для этого антивируса (обратное, к счастью, тоже верно: на любой алгоритм вируса всегда можно создать антивирус).

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.

# Заключение

В заключение хочется сказать, что компьютерные вирусы – не такая страшная вещь, если знать, как с ними бороться. Хоть они и мешают жизни современного человека, но, выполняя определённые действия, можно спокойно избежать контакта с ними.

# Источники

1. https://sites.google.com/site/antivirusnyeprogrammy34/komputernye-virusy/sposoby-protivodejstvia-komputernym-virusam
2. 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
3. http://sumk.ulstu.ru/docs/mszki/Zavgorodnii/10.1.html
4. http://mf.grsu.by/UchProc/livak/b\_protect/zkv\_1.htm
5. https://www.kaspersky.ru/resource-center/threats/computer-viruses-and-malware-facts-and-faqs
6. https://www.kaspersky.ru/resource-center/threats/a-brief-history-of-computer-viruses-and-what-the-future-holds