С прогрессом информационных технологий появляются всё новые и новые проблемы в плане защиты компьютерных систем. Одной из таких проблем являются вирусы. Довольно сложно представить себе, что неживая вычислительная техника может болеть также как и человек. Но это реально и чем совершеннее становятся технические средства, тем хитрее становятся и вирусы. Они являются болезнью, которую очень легко подхватить, но не так-то легко уничтожить. Вирусы портят жизнь компьютера и нашу жизнь, стирая самые нужные файлы; отсылают личные данные пользователя в Интернет без чьего-либо ведома; переворачивают всё содержимое ПК с ног на голову; маскируются под другими программами; создают новые файлы; хозяйничают во всех системах. Порой они уничтожают такие маленькие, но необходимые файлы, от которых «летит» вся операционная система. Вирусы не дают скачивать ссылки или вообще не пускают в Интернет; они тормозят работу процессора, выводят из строя акустическую или видеосистему; занимают лишнее место на диске и делают много чего другого. Самые современные системы антивирусной защиты не дают стопроцентной гарантии на то, что какой-либо умный вирус не залезет в компьютер. Многие вирусы при вылечивании и удалении забирают с собой и поражённый файл, и тогда приходится всё менять заново. Необходимо бороться с вирусами всеми возможными методами, особенно закрыть теневой рынок контрафактной продукции программного обеспечения, потому что в основном оттуда эта гадость и появляется

Компьютерный вирус – это самораспространяющийся в информационной среде программный код. Он может внедряться в исполняемые и командные файлы программ, распространяться через загрузочные секторы дискет и жестких дисков, документы офисных приложений, через электронную почту, Web-сайты, по другим электронным каналам. Проникнув в компьютерную систему, вирус может ограничиться безобидными визуальными или звуковыми эффектами, но может и вызвать потерю или искажение данных, утечку личной и конфиденциальной информации. В худшем случае компьютерная система, пораженная вирусом, окажется под полным контролем злоумышленника.

Сегодня компьютерам доверяют решение многих критических задач. Поэтому выход из строя компьютерных систем может иметь весьма тяжелые последствия,

вплоть до человеческих жертв (представьте себе, например, вирус в компьютерных системах аэродромных служб…).

На сегодняшний день известны десятки тысяч различных вирусов. Несмотря на такое изобилие, число типов вирусов, отличающихся друг от друга механизмом распространения и принципом действия, весьма ограниченно. Есть и комбинированные вирусы, которые можно отнести одновременно к нескольким типам. Вирусы представлены в хронологическом порядке появления.

Файловые вирусы.

Внедряясь в тело файлов программ .COM и .EXE, файловые вирусы изменяют их таким образом, что при запуске управление передается не зараженной программе, а вирусу. Вирус может записать свой код в конец, начало или середину файла. Получив управление, вирус может заразить другие программы, внедриться в оперативную память компьютера и т. д. Далее вирус передает управление зараженной программе, и та исполняется обычным образом.

Помимо .COM и .EXE файловые вирусы могут заражать программные файлы других типов – оверлеи MS-DOS (.OVL, .OVI, .OVR и другие), драйверы .SYS, библиотеки .DLL, а также любые файлы с программным кодом. Известны файловые вирусы для различных ОС – MS-DOS, Microsoft Windows, Linux, IBM OS/2 и т. д.

Загрузочные вирусы.

Загрузочные вирусы получают управление на этапе инициализации компьютера, еще до начала загрузки ОС. При заражении дискеты или жесткого диска загрузочный вирус заменяет загрузочную запись BR или главную загрузочную запись MBR. Исходные записи BR или MBR при этом обычно не пропадают (хотя бывает и иначе): вирус копирует их в один из свободных секторов диска.

При начальной загрузке компьютера BIOS считывает загрузочную запись с диска или дискеты, в результате чего вирус получает управление еще до загрузки ОС. Затем он копирует себя в конец оперативной памяти и перехватывает несколько функций BIOS. В конце процедуры заражения вирус загружает в память компьютера настоящий загрузочный сектор и передает ему управление. Далее все происходит, как обычно, но вирус уже находится в памяти и может контролировать работу всех программ и драйверов.

Комбинированные вирусы.

Очень часто встречаются комбинированные вирусы, объединяющие свойства файловых и загрузочных. В качестве примера можно привести широко распространенный когда-то файлово-загрузочный вирус OneHalf. Проникая в компьютер с ОС MS-DOS, этот вирус заражает главную загрузочную запись. Во время загрузки вирус постепенно шифрует секторы жесткого диска, начиная с самых последних секторов. Вирус OneHalf использует различные механизмы маскировки. Он представляет собой стелс-вирус и при распространении применяет полиморфные алгоритмы.

Вирусы-спутники.

Как известно, в MS-DOS и в Microsoft Windows различных версий существует три типа файлов, которые пользователь может запустить на выполнение. Это командные или пакетные файлы .BAT, а также исполняемые файлы .COM и .EXE. Когда вирус-спутник заражает файл .EXE или .BAT, он создает в этом же каталоге еще один файл с таким же именем, но с расширением .COM. Вирус записывает себя в этот COM-файл, который запускается до EXE-файла. При запуске программы первым получит управление вирус-спутник, который затем может запустить ту же программу, но уже под своим контролем.

Вирусы в пакетных файлах.

Существует несколько вирусов, способных заражать пакетные файлы .BAT. Они записывают свой двоичный код в тело пакетного файла после оператора комментария REM. При запуске такой пакетный файл копирует вирусный код в обычный исполняемый файл. Затем файл с вирусной программой запускается и удаляется. Получив управление, исполняемый файл вируса выполняет вредоносные действия и заражает другие пакетные файлы.

Шифрующиеся и полиморфные вирусы.

Некоторые вирусы шифруют собственный код, чтобы затруднить их обнаружение. Каждый раз, заражая новую программу, вирус использует для шифрования новый ключ. В результате два экземпляра такого вируса могут значительно отличаться друг от друга, даже иметь разную длину. Для шифрования применяются не только разные ключи, но и разные процедуры шифрования. Два экземпляра такого вируса не имеют ни одной совпадающей последовательности кода. Вирусы, способные полностью изменять свой код, получили название полиморфных.
Макрокомандные вирусы.

Файлы документов Microsoft Office могут содержать в себе небольшие программы для обработки этих документов, составленные на языке Visual Basic for Applications. Это относится и к базам данных Access, а также к файлам презентаций Power Point. Такие программы создаются с использованием макрокоманд, поэтому вирусы, живущие в офисных документах, называются макрокомандными. Макрокомандные вирусы распространяются вместе с файлами документов. Чтобы заразить компьютер таким вирусом, достаточно просто открыть файл документа в соответствующем приложении. Макрокомандные вирусы очень распространены, чему в немалой степени способствует популярность Microsoft Office. Они могут изменять зараженные документы, оставаясь незамеченными долгое время.

Самое интересное то что все вышеперечисленное это всего лишь маленькая часть, той обширной библиотеки вирусов , которая есть. Я считаю что для обеспечения своей безопасности не надо жалеть деньги на лицензионные программы, хоть и они не дают полной гарантии, что не появится новый вирус , который ваша программа даже не сможет распознать. Но с программой шанс защитить свой компьютер больше!

Список источников:

1. https://www.inetgramotnost.ru/
2. https://knep.ru/
3. https://welcom-comp.ru/antivir_pc/58-vidy-kompyuternyh-virusov.html