ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
БУРЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИМ. ДОРЖИ БАНЗАРОВА
Институт "Институт математики физики и компьютерных наук"
Кафедра "Общая и теоретическая физика"

Тема реферата

"Компьютерные вирусы"

Студент: Данилова Виктория Александровна гр. 01430М
Преподаватель: Жигжитов Алексей Олегович

Улан-Удэ
2024

Содержание

1 Введение

В современном цифровом обществе компьютерные вирусы стали одной из наиболее серьезных угроз для безопасности информации и непрерывности работы компьютерных систем. С каждым годом количество и разнообразие вирусов продолжают увеличиваться, и их воздействие становится все более разрушительным. От простых вирусов, наносящих ущерб файлам и программам, до сложных многокомпонентных малварей, способных перехватывать личную информацию и шифровать данные, компьютерные вирусы представляют собой серьезную угрозу как для индивидуальных пользователей, так и для организаций.

В данном реферате мы рассмотрим различные аспекты компьютерных вирусов, начиная с их определения и истории, и заканчивая методами защиты и превентивными мерами. Мы проанализируем различные виды вирусов, их характеристики и методы действия, а также рассмотрим последствия, которые они могут иметь для компьютерных систем и пользователей. В конечном итоге мы обсудим важность осведомленности о компьютерных угрозах и методов защиты, которые могут помочь минимизировать риски воздействия вирусов и обеспечить безопасность информации в цифровом мире.

Понимание природы и характеристик компьютерных вирусов является ключевым аспектом обеспечения кибербезопасности в нашей современной информационной эпохе. Давайте начнем наше исследование и углубимся в мир компьютерных вирусов, чтобы лучше защитить себя и свои данные от этой постоянно угрожающей опасности.

2 Общие сведения о компьютерных вирусах

2.1 Определение компьютерных вирусов

Компьютерные вирусы — это программы, разработанные для нанесения вреда компьютерным системам, а также для кражи или повреждения данных. Они внедряются в компьютерные системы без согласия их владельцев и способны распространяться на другие файлы или компьютеры, часто используя интернет или локальные сети.

Принято считать, что в первый раз слово «вирус» в значении программы применил Грегори Бенфорд в фантастическом рассказе «Человек в шрамах», который был опубликован в журнале Venture в мае 1970 года.

В общем и целом, компьютерный вирус получил свое название за принцип действия, аналогичный биологическим вирусам. А именно, сначала вирус проникает в клетку живого организма, после чего начинает размножаться, заражая другие клетки. Тогда, вирус перестает быть таким уж безобидным, человек (или животное) заболевает. Но стоит отметить, что вовремя «схваченный» вирус поддается лечению лучше, чем его «собрат» на более поздней стадии заражения. С компьютерными вирусам идентичная ситуация. Они точно также попадают в какую-либо программу, затем начинают заражать остальные. И в данной ситуации время также может сыграть не последнюю роль. При заражении компьютера вирусом важно его обнаружить, для этого следует знать основные признаки его проявления:

- прекращение работы или неправильная работа ранее успешно функционировавших программ;
- медленная работа компьютера;
- невозможность загрузки операционной системы;
- исчезновение файлов и каталогов или искажение их содержимого;
- изменение даты и времени модификации файлов;
- изменение размера 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.

Следует отметить, что вышеперечисленные явления необязательно вызываются присутствием вируса, а могут быть следствием других причин. Поэтому всегда затруднена правильная диагностика состояния компьютера. Заразиться компьютерным вирусом можно только в определенных случаях:

- запуск на компьютере исполняемой программы, заражённой вирусом;
- загрузка компьютера с диска (флеш-носителя, дискеты), содержащего загрузочный вирус;
- подключение к системе заражённого драйвера;
- открытие документа, заражённого макровирусом;
- установка на компьютере заражённой операционной системы.

Компьютер не может быть заражён, если:

- на него переписывались текстовые и графические файлы (за исключением файлов, предусматривающих выполнение макрокоманд);

- на нём производилось копирование с одной дискеты на другую при условии, что ни один файл с дискет не запускался;

- на компьютере производится обработка принесённых извне текстовых и графических файлов, файлов данных и информационных файлов (за исключением файлов, предусматривающих выполнение макрокоманд);

- переписывание на компьютер заражённого вирусом файла ещё не означает заражения его вирусом. Чтобы заражение произошло нужно либо запустить заражённую программу, либо подключить заражённый драйвер, либо открыть заражённый документ (либо, естественно, загрузиться с заражённой дискеты). Иначе говоря, заразить свой компьютер можно только в том случае, если запустить на нём непроверенные программы и (или) программные продукты, установить непроверенные драйвера и (или) операционные системы, загрузиться с непроверенной системной дискеты или открыть непроверенные документы, подверженные заражению макровирусами.

Попав в среду компьютера, вирус может и не вызвать довольно серьезных последствий (например, ограничиться безобидными визуальными или звуковыми эффектами), а может уничтожить или изменить (исказить) данные, также эта информация может стать «достоянием общественности». Но есть вариант и похуже: В худшем случае компьютер станет неисправным, и контролировать его сможет только автор вируса. Также стоит отметить, что вредоносные программы обычно занимают некоторое место, порой довольно большую часть оперативной памяти или накопителя информации. Потому вирусы относят к вредоносным программам.

У вирусов выделяют несколько стадий функционирования:

- латентная стадия (на данной стадии код вирусной программы располагается в системе, но никаких шагов не делает. Вирус является незаметным для пользователя. Обнаружить его можно только посредством сканирования системы);

- инкубационная стадия (на данной стадии код вируса активируется и начинает создавать свои копии, рассылая их по программам, файлам, всем данным, которые хранятся в памяти компьютера, также может вестись рассылка копий вирусной программы через электронную почту и так далее. Пользователь может его заметить, так как производительность компьютера падает, он начинает медленнее работать);

- активная стадия (на данной стадии вирус продолжает копировать и распространять свой код известными ему вариантами, начинает разрушительные действия, для осуществления которых и создан. Здесь вирусная программа становится очевидной для пользователя, потому что вредоносное ПО начинает выполнять свое предназначение – исчезают файлы, изменяется в негативную сторону функционирование сети, перестают быть активными некоторые программы, происходит поломка оборудования).

Существует множество разнообразных методов распространения вирусных программ. Но от наиболее часто используемых вирусов возможно защититься, соблюдая элементарные меры предосторожности.

Наиболее частые методы распространения вирусов представлены в таблице 1.

Таблица 1: Методы распространения вирусов и их характеристика

Метод	Характеристика
Флеш-накопители («флешки»)	Огромное число вирусных программ передается с помощью съёмных накопителей, в том числе фотоаппаратов, видеокамер, портативных MP3 и DVDплееров, а с не столь давних пор и через смартфоны и планшетные компьютеры, в которых также находятся «флешки».
Электронная почта	Чаще всего вирусные программы в письмах электронной почты маскируются под безвредные вложения в виде картинок, документов, музыки или ссылок на сайты. Иногда в письме на самом деле находятся только ссылки, безобидные на первый взгляд. При открытии послания они могут никак себя не проявить, то есть там может и не быть вредоносного кода, но при открытии подобной ссылки велика вероятность попадания на специально созданный веб-сайт, содержащий вирусный код.
Системы обмена мгновенными сообщениями	Аналогично уведомлениям в электронной почте, здесь распространяются ссылки как бы на фото, музыку либо программы, на самом деле являющиеся вредоносными программами. Делается это через ICQ, Viber, WhatsApp, Skype и другие программы мгновенного обмена сообщениями. В настоящее время нередки случаи распространения вирусов и с помощью SMS-сообщений.

Веб-страницы	Заражение может осуществляться и через вебсайты, а именно через рекламу, располагающуюся на страницах Интернета. При этом могут использоваться скрипты (процедура, выполняемая сервером по запросу, который отправляется с определенной страницы), ActiveX-компоненты (специальная технология, по которой создаются программы). Тогда используются «уязвимости» («дыры») — ошибки и недоработки ПО — программного обеспечения компьютера пользователя или «уязвимости» того же программного обеспечения владельца сайта. Второй случай является более опасным, потому что тогда заразиться рискуют и ни в чем не повинные сайты с большим потоком посетителей, с которых в свою очередь могут заразиться и компьютеры этих же посетителей.
Интернет и локальные сети («черви»)	«Черви» — это разновидность вирусов, которые проникают в компьютер без вмешательства пользователя. «Черви» эксплуатируют вышеупомянутые «дыры», или «уязвимости» программного обеспечения, чтобы проникнуть во внутреннюю среду компьютера. Именно эти слабые места программного обеспечения дают машинному коду возможность загрузиться, так вирус-червь оказывается в операционной системе и начинает заражать другие компьютеры посредством локальной или глобальной сети. Чаще всего такой вирус используется для рассылки спама (рассылка коммерческой и иной рекламы индивидам, не изъявлявшим желания их получать) или для DDoS-атак (вирусные атаки, цель которых заключается в выведении компьютера из строя).

2.2 Классификация компьютерных вирусов

По принципу своего функционирования вирусы можно разделить на несколько типов:
- вирусы-паразиты;
- вирусы-репликаторы;
- трояны;
- вирусы-невидимки;
- самошифрующиеся вирусы;
- матирующиеся вирусы;
- "отдыхающие"вирусы.

Данные вирусы и их признаки представлены в таблице 2.

Таблица 2: Классификация вирусов по принципу функционирования

Вирус	Характеристика
Вирусы-паразиты	Это вирусы, которые работают с файлами программ и которые неполностью выводят их из строя. Такие вирусы нетрудно обнаружить и ликвидировать. Тем не менее, в основном, файлоноситель восстановлению не полежит.

Вирусы-репликаторы	Это вирусные программы, целью которых является быстрое создание собственных копий и их распространение по всем возможным местам хранения данных и каналам сообщения. Сами по себе вирусы-репликаторы часто не совершают никаких разрушительных для операционной системы действий, а являются «перевозчиком» для других видов вредоносного кода.
Трояны	Это вирусы, получившие свое название в честь знаменитого “Троянского коня”, потому что действуют подобным образом. Этот вид вирусов стягивает свои модули в одно место под модули действующих программ, создавая файлы со схожими названиями и характеристиками, меняют записи в системном реестре, изменяя ссылки рабочих модулей программ на свои, вызывающие модули вируса. Разрушительная деятельность ведет к ликвидации данных пользователя, рассылке спама и полному контролю злоумышленника за действиями владельца компьютера. Трояны не обладают способностью к репликации. Их довольно сложно обнаружить, потому что обычно сканирования файловой системы мало.

По среде обитания вирусы можно разделить на такие виды:
- загрузочные вирусы;
- файловые вирусы;
- файлово-загрузочные вирусы;
- сетевые вирусы;
- документные вирусы.

Классификация вирусов и их характеристики по среде обитания представлены в таблице 3.

Таблица 3: Классификация вирусов и их характеристики по среде обитания

Вирус	Характеристика
Загрузочные вирусы	Внедряются в накопители информации, а именно в жесткие диски и внешние запоминающие устройства. Когда операционная система загружается, вирус активируется. Он нарушает работу загрузчика операционной системы, в результате она перестает работать или в файлах возникают ошибки, что делает их недоступными.

Файловые вирусы	Обычно они проникают в исполнительные модули программ (файлы, с помощью которых запускается та или иная программа), благодаря чему они могут активироваться, когда запускается программа, это влияет на функциональность данной программы. Файловые вирусы реже проникают в операционную систему, исполнительные пакетные файлы, файлы реестра Windows, файлы сценариев, файлы драйверов. Проникновение ведется посредством изменения кода атакуемого файла или создания его модифицированной копии. Когда вирус находится в файле и имеет непосредственный доступ к нему, он начинает активироваться, если пользователь или сама ОС проявляет инициативу. Файловые вирусы относятся к одним из самых распространенных видов компьютерных вирусов.
Файлово-загрузочные вирусы	Они сочетают в себе способности двух вышеупомянутых видов вирусов, потому являются более опасными.
Сетевые вирусы	Их распространение ведется через сетевые службы и протоколы (например, с помощью рассылки почты, доступа к файлам через службы локальных сетей). Эти факторы делают сетевые вирусы крайне опасными, потому что заражение ведется не по одной локальной сети, а распространяется на другие сети с помощью каналов связи
Документные вирусы (или макровирусы)	Заражают файлы современных офисных систем (Microsoft Office, Open Office...) с помощью способности использования в этих системах макросов. Макрос – это сокращенное название макрокоманды, набор команд (операций), которые можно записывать и потом выполнять. Макросы очень удобны для выполнения повторяющихся и сложных операций. Именно макрос и является целью макровирусов.

По методу существования в компьютерной среде вирусы делятся на такие виды:
- резидентные;
- нерезидентные.
Виды вирусов и их описание по методу существования представлены в таблице 4.

Таблица 4: Классификация вирусов по методу существования в компьютерной среде и их признаки

Вирус	Характеристика
Резидентный вирус	Вызывается посредством запуска программы и сохраняется в памяти даже по завершении. Данный вирус способен активировать дополнительные операции в памяти компьютера, при этом также расходуются ресурсы. Резидентный вирус заражает и другие активные программы, при этом ухудшается их работоспособность. Также он способен прослеживать действия пользователя, сохраняя информацию о введенных паролях, посещенных сайтах и т.д.

Нерезидентный вирус	Обладает всеми теми свойствами, что и резидентный, но с одним отличием: нерезидентный активен, только пока функционирует зараженная программа.

По степени воздействия вирусы можно разделить на такие разновидности:
- неопасные;
- опасные;
- особо опасные.

Классификация вирусов по степени воздействия и их свойства описаны в таблице 5.

Таблица 5: Классификация вирусов по степени воздействия и их признаки

Вирус	Характеристика
Особо опасные	Могут привести к потере программ, уничтожению данных, стиранию информации в системных областях диска.
Опасные вирусы	Способны приводить различным нарушениям в работе компьютера.
Неопасные вирусы	Не особо влияют на работоспособность компьютера, но уменьшают объем свободной оперативной памяти и памяти на дисках, как правило, проявление таких вирусов становится заметно в каких-либо графических или звуковых эффектах.

Но далеко не все компьютерные вирусы являются крайне опасными. Некоторые из них и вовсе не влекут за собой серьезных последствий. Например, они могут завершить работу некоторых программ, отображать определенные визуальные эффекты, воспроизводить звуки, открывать сайты, или просто снижать производительность компьютера, занимая много памяти. И такие вирусы доминируют в современном мире. Но существуют и на самом деле опасные вирусы, которые способны уничтожить данные пользователя, документы, выводить из строя операционную систему и т.д. Поэтому очень важно уметь защищаться от вирусов.

3 Методы защиты информации от вирусов

3.1 Профилактические мероприятия

Существует несколько способов, с помощью которых мы можем защитить нашу систему и данные от вирусного воздействия:

1. **Поддерживайте свое программное обеспечение в актуальном состоянии**

Компании-разработчики программного обеспечения, такие как Microsoft и Oracle, регулярно обновляют свое программное обеспечение для устранения ошибок. Неактуальность версии программного обеспечения может быть использовано вирусом для возможности заражения компьютера.

2. **Не переходите по ссылкам в электронных письмах**

Хорошее эмпирическое правило заключается в том, что если вы не узнаете отправителя электронного письма, то не нажимайте ни на какие ссылки в письме.

3. **Используйте бесплатное или платное антивирусное программное обеспечение**

Вам не нужно покупать программное обеспечение для защиты вашего компьютера или годовую подписку, чтобы позаботиться о новейшей защите от вирусов. Для пользователей Windows Microsoft Security Essentials бесплатна. Avast — это еще одна бесплатная антивирусная программа.

4. **Резервная копия данных**

Если у вас нет защиты системы, то вы должны периодически делать резервную копию своих данных. Три основных варианта резервного копирования: Внешний накопитель, Онлайн-служба резервного копирования, Облачное хранилище. Используйте такие услуги, как Google drive, Google docs для хранения файлов. Некоторые облачные хранилища имеют определенный бесплатный объем хранения данных. Виртуальное хранилище — это ресурс для сохранения ваших данных.

5. **Пароль**

В то время как некоторые люди используют эквивалентный пароль для всего, избегайте этой практики. Длина пароля должна составлять не менее восьми символов. Надежный пароль, состоит из букв, цифр и символов. Периодически меняйте свой пароль.

6. **Брандмауэр**

Если в вашей системе запущено антивирусное программное обеспечение, то это не значит, что у вас есть брандмауэр. Компьютеры на базе ОС Windows и IOS имеют встроенное программное обеспечение брандмауэра. Убедитесь, что он включен.

7. **Блокировщик всплывающих окон**

Веб-браузеры имеют возможность предотвращать всплывание окон. Вы можете использовать Add Blocker, чтобы заблокировать вредоносную и навязчивую рекламу на веб-сайтах.

3.2 Антивирусное программное обеспечение

Антивирусное программное обеспечение обнаруживает и удаляет вирусы и другие вредоносные программы, такие как черви, трояны, рекламное ПО и многое другое. Это программное обеспечение предназначено для использования в качестве превентивного подхода к кибербезопасности, чтобы остановить угрозы до того, как они попадут на ваш компьютер и вызовут проблемы.

Антивирусное программное обеспечение работает, сканируя входящие файлы или код, который передается через сетевой трафик. Компании, которые создают это программное обеспечение, составляют обширную базу данных уже известных вирусов и вредоносных программ и регулярно обновляют ее. Когда файлы, программы и приложения передаются на ваш компьютер, антивирус сравнивает их со своей базой данных, чтобы найти совпадения. Совпадения, похожие или идентичные базе данных, изолируются в карантин, сканируются и удаляются. В режиме реального времени, когда вы просматриваете веб-страницы, отправляете электронные письма, смотрите потоковое видео или делаете что-либо еще в Интернете, программное обеспечение предупредит вас, чтобы вы не нажимали на какие-либо веб-сайты или файлы, которые могут представлять угрозу вашей безопасности в Интернете.

По данным исследовательского портала US News 360 Reviews на 4 апреля 2024 год составлен рейтинг популярных антивирусных программ для Windows 11 и Windows 10:

1. Bitdefender. Цена от 40 долларов и выше. Присутствует бесплатная пробная версия.
2. AVG Free Antivirus. Бесплатный.
3. Malwarebytes Премиум. Цена от 40 долларов и выше. Присутствует бесплатная пробная версия.
4. Norton 360 Select с Lifelock Select. Цена от 100 долларов за 10 устройств и выше. Бесплатная версия отсутствует.
5. Eset Mobile Security Premium. Цена от 13 долларов и выше. Присутствует базовая бесплатная версия.

4 Заключение

В современном цифровом мире компьютерные вирусы представляют собой серьезную угрозу для безопасности информации и непрерывности работы компьютерных систем. От простых вирусов-червей, способных автоматически распространяться через сети, до сложных рансомваров, требующих выкуп за разблокировку зараженных данных, вирусы могут привести к серьезным материальным потерям и нарушениям конфиденциальности.

Однако существуют различные методы защиты от компьютерных вирусов, которые могут помочь минимизировать риски воздействия и обеспечить безопасность данных и компьютерных систем. Это включает в себя использование антивирусного программного обеспечения, регулярное обновление программ и операционной системы, а также осторожное поведение в сети.

Важно осознавать угрозу компьютерных вирусов и принимать соответствующие меры для защиты себя и своих данных. Обучение пользователям безопасному поведению в интернете, регулярное резервное копирование данных и использование многоуровневой защиты могут значительно снизить риск заражения компьютера вирусами и другими вредоносными программами.

Только путем совместных усилий и постоянного внимания к кибербезопасности мы можем обеспечить безопасное и надежное функционирование в цифровой эпохе.

Список литературы

[1] Афанасьева Д.В. - Компьютерные вирусы: специфика и противодействие // Наука, образование и культура. 2019. №. 3 (37). С. 11–12.

[2] Атамкулова М. Т., Саримсаков А. А. Компьютерные вирусы и антивирусные программы //Известия Ошского технологического университета. 2016. Т. 2. С. 136–140.

[3] Ганижева Н. Ж. Компьютерные вирусы и антивирусные программы //Молодой ученый. 2021. №. 33. С. 3–5.

[4] Зенкин Д. В., Касперский Е. В. Компьютерные вирусы: происхождение, реальная угроза и методы защиты, режим доступа: свободный / [Электронный ресурс] URL: https://www.nkj.ru/archive/articles/7889/ (дата обращения: 20.04.2024).

[5] Попов Илья Олегович, Марунько Анна Сергеевна, Петров Олег Игревич, Олейник Анастасия Александровна Вирусы и антивирусные программы в информационной безопасности // Научные записки молодых исследователей. 2020. №4. URL: https://cyberleninka.ru/article/n/virusy-i-antivirusnye-programmy-v-informatsionnoy-bezopasnosti (дата обращения: 20.04.2024).

[6] Козлов Захар Сергеевич КОМПЬЮТЕРНЫЕ ВИРУСЫ И АНТИВИРУСЫ // Столыпинский вестник. 2022. №4. URL: https://cyberleninka.ru/article/n/kompyuternye-virusy-i-antivirusy (дата обращения: 20.04.2024).