Компьютерные вирусы и системы им противодействия

Кушнаренко Александр Игоревич, студент

АУ «Сургутский политехнический колледж»

Преподаватель: Воробьева О.Н.

Почему возникают компьютерные вирусы? Как уберечь свой компьютер от них? Являются ли антивирусные программы эффективным средством защиты и, какие из них, лучшие? Вот такими вопросами можно «очертить» круг проблем, возникающий перед каждым пользователем компьютера.

**Актуальность работы:** является изучение компьютерных вирусов и их влияние на работоспособность компьютеров.

Информация в современном обществе является на данный момент одним из самых ценных продуктов. Поэтому проблемы сохранения и [защиты информации](https://pandia.ru/text/category/zashita_informatcii/) являются очень важными и волнуют каждого от школьника до президента страны.

**Цель работы:** изучить способы внедрения вирусов, их влияние на производительность компьютера, а также определение способов защиты от вирусных программ.

**Гипотеза**: существующие антивирусные программы способны защитить информацию, хранящуюся на компьютере.

**Объектом:** компьютерные вирусы.

**Предметом:** методы борьбы с компьютерными вирусами.

Для достижения поставленной цели нам необходимо решить следующие **задачи:**

- определить классификацию вирусов по способам проникновения их в компьютер;

- изучить влияние вирусов на работу компьютера и безопасность личных данных;

- выделить методы защиты от компьютерных вирусов;

- сделать выводы.

Мы предполагаем, что существующие антивирусные программы способны защитить информацию, хранящуюся на компьютере. И если предположить, что это так, то созданный нами тест-вирус должен быть определен, хотя бы одной из них.

Мы предполагаем, что созданный нами тест-вирус должен быть определен, хотя бы одной из существующих ныне антивирусных программ, способных защитить информацию, хранящуюся на компьютере,

1. **Компьютерные вирусы.**

Компьютерный вирус – это небольшая вредоносная программа, которая самостоятельно может создавать свои копии и внедрять их в программы (исполняемые файлы), документы, загрузочные сектора носителей данных и распространяться по каналам.

Когда такая программа начинает работу, то сначала управление получает вирус. 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.).

При заражении компьютера вирусом важно его обнаружить, для этого следует знать основные признаки его проявления 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;
* прекращение работы или неправильная работа ранее успешно функционировавших программ;
* медленная работа компьютера;
* невозможность загрузки операционной системы.

**2. Классификация вирусов**

Вирусы можно делить на классы по разным признакам. На схеме отображены основные признаки и классы компьютерных вирусов.

**Классификация вирусов:**

1.    По среде обитания различают вирусы сетевые, файловые, загрузочные и файлово-загрузочные.

2.    По способу заражения выделяют резидентные и нерезидентные вирусы.

3.    По степени воздействия вирусы бывают неопасные, опасные и очень опасные;

4.    По особенностям алгоритмов вирусы делят на паразитические, репликаторы, невидимки, мутанты, троянские, макро-вирусы.

Возможно деление вирусов по признаку вероломности: вирусы, моментально поражающие компьютер, форматируют жесткий диск, портят таблицу размещения файлов, портят загрузочные сектора, стирают так называемое Flash-ПЗУ (где находится BIOS) компьютера (вирус «Чернобыль»).

Вирус «Чернобыль - резидентный вирус (заражает память компьютера и перехватывают все обращения ОС к объектам, пригодным для заражения), работающий в операционной системе Виндовс.

**3. Способы маскировка вирусов**

Существуют способы маскировок и защит, применяемых вирусами против нас рядовых пользователей и антивирусных программ.

В соответствии со способами маскировки различают:

1. Немаскирующиеся вирусы;
2. Самошифрующиеся вирусы;
3. Стелс-вирусы.

При создании копий для маскировки могут применяться следующие технологии:

- шифрование — вирус состоит из двух функциональных кусков: собственно вирус и шифратор. Каждая копия вируса состоит из шифратора, случайного ключа и собственно вируса, зашифрованного этим ключом.

- метаморфизм — создание различных копий вируса путем замены блоков команд на эквивалентные, перестановки местами кусков кода, вставки между значащими кусками кода «мусорных» команд, которые практически ничего не делают.

**4. Профилактика и борьба с компьютерными вирусами.**

Для защиты от вирусов можно использовать:

1. общие средства защиты информации, которые полезны также как страховка от физической порчи дисков, неправильно работающих программ или ошибочных действий пользователей;
2. профилактические меры, позволяющие уменьшить вероятность заражения вирусом;
3. специализированные программы для защиты от вирусов.

Существуют две основные разновидности этих средств:

- копирование информации — создание копий файлов и системных областей дисков;

- разграничение доступа предотвращает несанкционированное использование информации, в частности, защиту от изменений программ и данных вирусами, неправильно работающими программами и ошибочными действиями пользователей.

Принимаемые меры, которые позволяют уменьшить вероятность заражения компьютера вирусом, а также свести к минимуму ущерб от заражения вирусом, если оно все-таки произойдет.

1. Обновлять архивные и эталонные копии используемых пакетов программ и данных.
2. Следует устанавливать защиту от записи на архивных дискетах.
3. Не следует заниматься нелицензионным и нелегальным копированием программного обеспечения с других компьютеров. На них может быть вирус.
4. Все данные, поступающие извне, стоит проверять на вирусы, особенно файлы, «скачанные» из Интернета.
5. На время обычной работы, не связанной с восстановлением компьютера, стоит отключить загрузку с дискеты. Это предотвратит заражение загрузочным вирусом.
6. Используйте программы – фильтры для раннего обнаружения вирусов.
7. Обновляйте базу антивирусных программ.
8. Не допускайте к компьютеру сомнительных пользователей.

**Заключение**

Компьютерные вирусы во всем мире наносят громадный ущерб. Эти маленькие вредоносные программы живут по трём правилам – Размножаться, Скрываться и Портить. И какие потрясения бывают, когда однажды пропадают данные, которые собирались и накапливались может не один год....

Чтобы этого не произошло, нужно знать о существовании компьютерных вирусов и уметь защищать свои данные.

Таким образом, в наш век высоких технологий, когда пользователь основную массу времени проводит в Интернете и одной из актуальных проблем являются компьютерные вирусы. Технологии совершенствуются с огромной скоростью, как и вирусы. Причем порой при заражении довольно сложно понять, что конкретно случилось с компьютером.

При изучении темы, привели классификацию вирусов, можно делить на классы по разным признакам. На схеме мы отобразили основные признаки и классы компьютерных вирусов.

Рассмотрели программы, которые проникают в компьютер и выполняют вредоносные функции это троянские программы, логические бомбы, программы – черви.

После массового распространения вирусов появилось огромное количество антивирусных программ.

Обеспечивать эффективную защиту в режиме реального времени. Производить проверку всех файловых операций, сообщений электронной почты, данных и программ, получаемых из Интернета. Защищать наш компьютер даже от неизвестных вирусов. Уметь проверять и лечить архивированные файлы. Давать возможность ежедневно обновлять антивирусные базы.

Несмотря на то, что общие средства защиты информации очень важны для защиты от вирусов, все же их одних недостаточно. Необходимо применять специализированные программы для защиты от вирусов.

Рассмотрели шесть антивирусных программ их достоинства и недостатки. Это **Kaspersky, Аvast, Dr.Web, ESET NOD32, AVG, McAfee**.

Каждый из рассмотренных антивирусов по тем или иным показателям заслужил свою популярность, но явного лидера среди них выявить невозможно.

Для своего компьютера, самый лучший антивирус следует подбирать, исходя из функциональности, самостоятельно протестировав несколько продуктов. Многие разработчики антивирусных программ предлагают возможность использовать бесплатную пробную версию (от 30 до 90 дней). Это позволит и ознакомиться с продуктом, понять, какой антивирус самый лучший именно для вас.

К сожалению, на данный момент универсальной антивирусной программы не существует. Существующие антивирусные программы способны защитить информацию, хранящуюся на компьютере. Но ни одна из них не может гарантировать нам 100% защиты от вирусов.

Антивирус вещь хорошая, но некоторые пользователи умудряются заразить компьютер даже с ним, поэтому, нужно помнить прописную истину пользователя: «Если не знаешь, что это, откуда и для чего, лучше не открывай!».

**Список использованной литературы**

1. Новожилов, О. П.Информатика: учебник для СПО / О. П. Новожилов. — 3-е изд., пер. и доп. — Москва : Юрайт, 2019. — 620 с. — Текст : электронный // ЭБС Юрайт : [сайт]. — URL: <https://biblio-online.ru/bcode/441892> (дата обращения: 01.10.2019).
2. Филимонова Е. В. Информатика и информационные технологии в профессиональной деятельности. Учебник. М.: Юстиция, 2019. 216 с.
3. Козлов Д. А., Парандовский А. А., Парандовский А. К. Энциклопедия компьютерных вирусов.- М: Солон-Р, 2019.- 458 с.

Интернет – ресурсы:

[http://www.viruslist.com](https://infourok.ru/go.html?href=http%3A%2F%2Fwww.viruslist.com%2F) - Все угрозы.

[http://www.bytemag.ru](https://infourok.ru/go.html?href=http%3A%2F%2Fwww.bytemag.ru%2F) – BYTE/Россия – Что нужно знать о компьютерных вирусах.

[http://antivibest.ru](https://infourok.ru/go.html?href=http%3A%2F%2Fantivibest.ru) – Антивирусные программы.

http://www.academ.org - Мостовой Д.Ю. «Современные технологии борьбы с вирусами»

http://journal-shkolniku.ru - Моисеенков И. «Безопасность компьютерных систем»

http://prontocom.ru - А.В. Михайлов «Компьютерные вирусы и борьба с ними»