|  |  |
| --- | --- |
| **Выполнил**  **Студент гр. 3530904/10002** | **И.С. Тампио** |
| **Руководитель**  **Доцент, к.т.н.** | **В.С. Тутыгин** |

1. Введение – зачем, почему, цель работы

Компьютеры является неотъемлемой частью жизни как отдельного пользователя, так и больших корпораций. Любые неисправности, возникающие в их работе, могут привести к крупным денежным и временным потерям. Помимо простых технических неполадок, к таким неисправностям могут приводить компьютерные вирусы. Их последствия ещё более деструктивны. Для юридических лиц, конфиденциальные данные или коммерческая тайна могут уйти злоумышленникам, что подорвёт доверие к той или иной компании. Для отдельного пользователя заражение компьютера вирусом чревато материальными потерями и неудобствами в работе с компьютерами, потерей личных файлов. В связи с этим важно понимать, чем являются вирусы и как с ними бороться. Целью этой работы является рассказать о том, как можно бороться с вирусами.

1. Вирусы – определение – что такое?

Формального определения того, чем является компьютерный вирус не дано до сих пор, но если их обобщить, то вредоносным ПО можно назвать любую программу, совершающую нежелательные для пользователя действия.

1. Как вирус попадает на компьютер пользователя?

Давайте рассмотрим, каким образом вирус попадает на компьютер пользователя. Зачастую злоумышленник обманом заставляет скачать вредонос на компьютер – будь то через поддельные письма с интересным для пользователя заражённым содержимым или путём подделывания официальных сайтов загрузки приложений.

1. Что вирус может сделать с компьютера пользователя?

После того, как вирус запускается, и ничего не мешает его исполнению, компьютер можно считать заражённым. Действия, совершаемые вирусом бывают совершенно разные:

* 1. Реклама

Вирус добавляет рекламу в бразуер, систему, тем самым злоумышленник получает прибыль с показов рекламы.

* 1. Вирусы-шпионы

Наиболее распространены среди вирусов-шпионов вирусы-кейлоггеры, которые считывают ввод пользователя, в том числе данные кредитных карт и аккаунтов, и отправляют его пользователям.

* 1. Вирусы-вымогатели

Такие вирусы блокируют систему, не позволяя пользователю ничего сделать и заставляют его отправить деньги. Стоит сказать, что отправка денежных средств – рискованная, поскольку не гарантирует разблокировку устройства.

* 1. Рут-киты \ Боты \ Вирусы удалённого доступа

Такие вирусы делают компьютер частью сети заражённых компьютеров злоумышленника, которую тот может использовать для самых различных целей. Одними из них являются добыча криптовалюты и DDOS атаки.

* 1. Черви

Вирусы-черви распространяют сами себя в компьютерных сетях, посылая свои копии на другие компьютеры по локальной сети или с помощью аккаунтов пользователя по почте и в социальных сетях.

1. Как лечить компьютер?

Существует миф, что вирусы могут заразить компьютер навсегда, что неверно, поскольку вирус существует только на жёстком диске компьютера. Есть несколько способов вылечить компьютер от вирусов.

* 1. Переустановка системы

Переустановка системы позволяет гарантированно избавиться от вирусов, и, к сожалению, всего того, что осталось на заражённом компьютере. Если файлы не зашифрованы, то необходимые данные можно сохранить. Это хороший способ вылечить компьютер, но увы, он времязатратен.

* 1. Деинсталляция рекламных программ

В частных случаях, вирусы, встраивающие рекламу в браузер оставляют для пользователя деинсталлятор, позволяющий удалить вирус. В таком случае можно просто запустить программу деинсталлятор и удалить вирус.

* 1. Использование антивируса

Использование антивируса плохо тем, что оно нагружает систему, однако для обычного пользователя это идеальный метод защиты от вирусов, не требующий особых навыков. Более того – наличие антивируса на компьютере – стандарт информационной безопасности, требуемый государством. Антивирус сам найдёт вирусы и удалит их, защитит систему от подозрительных файлов.

1. Превентивные меры предосторожности – повышение уровня цифровой грамотности сотрудников компании, инструктажи

Несмотря на способы лечения и защиты от компьютерных вирусов. Самой действенной защитой является образованность пользователя. Если не скачивать приложения с неофициальных сайтов и быть чуть более внимательным при работе в интернете – можно спокойно обойтись без заражения компьютера.

1. Заключение – какой антивирус рекомендую поставить и о излишних мерах предосторожности.

В заключение хочется сказать, что излишняя предосторожность тоже ведёт к убыткам, поскольку в таком случае постоянные проверки излишне нагружают систему, и ведут к общим денежным и временным убыткам. Моей личной рекомендацией для неумелого пользователя будет установить Dr. Web, поскольку он является достаточно легковесным антивирусом, который выполняет свою задачу на ура. Спасибо за внимание.