3. Энергетическая проблема–[Электронный ресурс] / Режим доступа к данным: http://www.grandars.ru/student/mirovaya-ekonomika/energeticheskaya-problema.html/ (Дата обращения: 24.05.2018).

4. Основные проблемы энергетики и возможные способы их решения. текст научной статьи по специальности «энергетика»–[электронный ресурс] / режим доступа к данным: https://cyberleninka.ru/article/n/osnovnye-problemy-energetiki-i-vozmozhnye-sposoby-ih-resheniya (Дата обращения: 24.05.2018).

РАЗНОВИДНОСТИ КОМПЬЮТЕРНЫХ ВИРУСОВ И СПОСОБЫ ЗАЩИТЫ ОТ НИХ

Пырч Денис (Запорожье, Украина)

Актуальность темы исследования. Каждый день появляется всё больше новых вирусов, которые могут причинить вред не только информации, содержащейся на компьютере, но также повредить сам компьютер. По этой причине необходимо знать, какие бывают признаки заражения компьютера, какие существуют разновидности вирусов и способы защиты компьютера от них.

Цели исследования – изучить понятие, виды, признаки заражения, а также способы противостояния компьютерным вирусам.

Проблемная ситуация. Проблемная ситуация в том, что почти каждый человек в современной мире пользуется компьютером, но к сожалению не знает или плохо осведомлён о способах защиты от компьютерах вирусов, что в свою очередь привод к нанесению вреда компьютеру и информации, которая на нём хранится.

Методы и методология исследования. Для исследования темы компьютерные вирусы и способы защиты от них использовались методы анализа, синтеза и сравнения информации.

Результат исследования. Компьютерный вирус — вид вредоносного программного обеспечения, способного создавать копии самого себя и внедряться в код других программ, системные области памяти, загрузочные секторы, а также распространять свои копии по разнообразным каналам связи[1].

Основные представители компьютерных вирусов:

1. Червь — это вредоносная программа, которая занимается копированием самой себя и тем самым захламляет свободное место на жестком диске пользователя.

2. Троянский конь — вирус, который открывает доступ к компьютеру жертвы для удаленного манипулирования.

3. Программы-шпионы — они занимаются кражей паролей пользователя и отправкой их автору вируса.

4. Зомби-вирусы — по сути это черви или троянские кони, которые объединены в группу (ботнет) для того, чтобы массово выполнять действия с компьютеров жертв.

5. Вирусы-вымогатели (баннеры) — в отличии от большинства вирусов, которые пытаются скрыть свое присутствие на компьютере пользователя, эти вирусы действуют наоборот — заявляют о себе, не давая жертве получить доступ в свою операционную систему.

6. Шифровальщики — Заражение часто происходит при открытии пользователем вложения в электронном письме. Сначала на компьютер загружается программа, которая скачивает сам вирус и устанавливает его в системе. После этого она удаляется, и за дело берется сам вирус-шифровальщик, который шифрует важные файлы. После этого рядом со всеми зашифрованными файлами появляется инструкция в которой указано, как перевести деньги за расшифровку.

7. Malware — как правило программы-паразиты (плагины к браузерам и т. п.) целью которых является постоянная навязчивая демонстрация пользователю сторонней рекламы. Могут открывать дополнительные окна в браузере (обычно — со все той же рекламой)[2].

Признаки заражения компьютера: вывод на экран непредусмотренных сообщений или изображений, подача непредусмотренных звуковых сигналов, произвольный запуск на компьютере программ, частые «зависания» и сбои в работе компьютера, медленная работа компьютера при запуске программ, исчезновение или изменение файлов и папок, частое обращение к жесткому диску, «зависание» или неожиданное поведение браузера[3].

Выводы. Проблемы от вирусов могут быть самые разнообразные: некоторые можно устранить, некоторые – нет. Почти всех этих сложностей можно избежать, или хотя бы свести к минимуму вероятность их появления.Для этого нужно следовать нескольким простым правилам:

1. Использовать новейшее и лицензионное программное обеспечение;

2. Использовать современное антивирусное программное обеспечения с актуальными антивирусными базами;

3. Не попадаться на уловки мошенников;

4. Не забывайте делать резервные копии важных данных и хранить их отдельно[2].

Ключевые слова: компьютерные вирусы, антивирусы.

Список литературы:

1. Компьютерный вирус – [Электронный ресурс] / Режим доступа к данным: https://ru.wikipedia.org/wiki/Компьютерный_вирус (Дата обращения: 18.05.2018).

2. АНТИВИРУСЫ — ДЕРЖИМ ДАННЫЕ ПОД НАДЕЖНОЙ ЗАЩИТОЙ! – [Электронный ресурс] / Режим доступа к данным: http://adeptis.ru/infoantivirus.html(Дата обращения: 18.05.2018).