Согласовано
Совет КГБПОУ СИЭК
Протокол № 1
от «10» июня 2014 г

Утверждаю:
Директор КГБПОУ СИЭК
_____ Л.М. Шевандронова
«10» июня 2014 г.

Рабочая инструкция пользователя ПК по обеспечению информационной безопасности при работе с электронными документами (файлами) в КГБПОУ СИЭК

г. Спасск – Дальний
2014

Данная инструкция предназначена для предупреждения следующих основных угроз безопасности электронных документов (далее - файлов) на компьютерах пользователей:

а) Порча/потеря/нарушение конфиденциальности данных в результате изменения/удаления файла по неосторожности либо намеренного просмотра/изменения/удаления файла посторонним лицом.

б) Порча/потеря/нарушение конфиденциальности данных в результате заражения файлов пользователя, а также файлов программ и операционной системы вирусными программами.

Данная инструкция предусматривает следующие меры, предпринимаемые пользователем для обеспечения безопасности процессов хранения, передачи и обработки файлов на компьютере пользователя:

1. Обеспечение безопасности работы в сети Интернет.

1.1 Перед выходом в сеть Интернет пользователь должен убедиться, что на его компьютере установлена и включена антивирусная программа, содержащая антивирусные базы, обновлённые не ранее чем 2 недели назад. На рисунке 1 приведён пример значка программы «Антивирус Касперского Personal 5.0» в системном лотке. При более раннем сроке обновления антивирусных баз пользователь должен обратиться к инженеру-программисту для обновления баз.

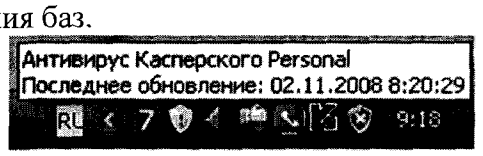

Рисунок 1. При наведении курсора мыши на значок в виде красной буквы К появляется подсказка о дате обновления антивирусных баз.

1.2 При выдаваемых антивирусной программой сообщениях о сетевых атаках пользователь в отсутствие инженера-программиста должен поставить отметку в поле «Не показывать это сообщение в следующий раз» и нажать кнопку ОК (см. рисунок 2).

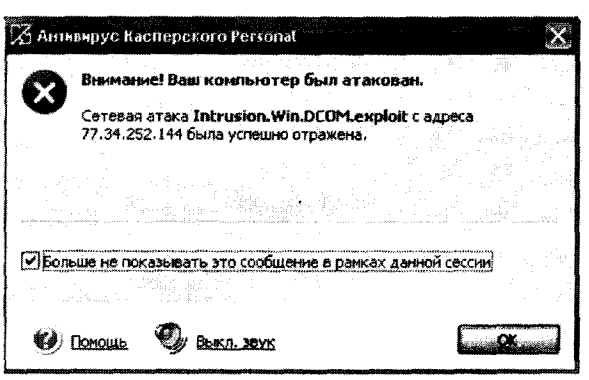

Рисунок 2. Сообщение о сетевой атаке

1.3 Все файлы, копируемые пользователем на свой компьютер из сети Интернет, должны быть проверены антивирусной программой во избежание проникновения в компьютер вирусных программ, способных уничтожить важные данные пользователя. Для этого пользователю необходимо кликнуть правой кнопкой мыши на закачанном из Интернета файле и выбрать пункт «Проверить на вирусы» (рисунок 3). Если антивирусная программа не обнаружила вирусов в проверяемом файле, то файл условно считается безопасным.

1.4 При выдаваемых программой сообщениях об обнаруженном вирусе (рисунок 4) пользователю необходимо обратиться к инженеру-программисту.

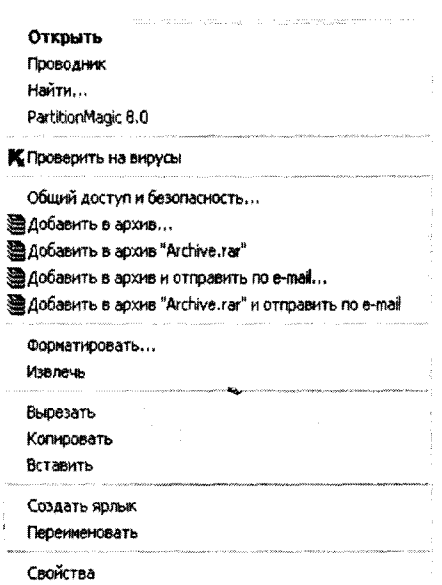

Рисунок 3. Контекстное меню проверяемого объекта

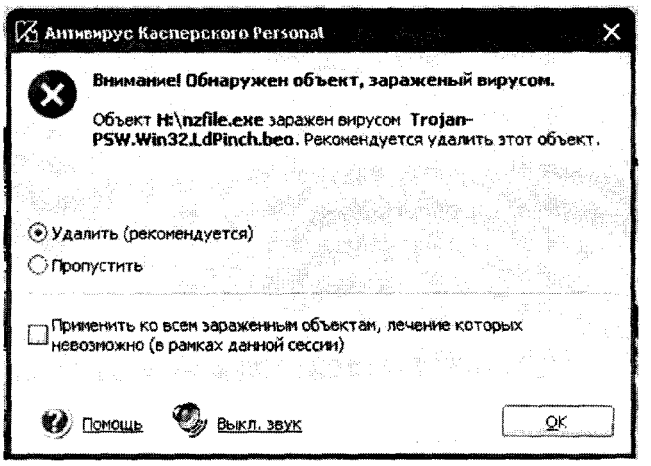

Рисунок 4. Сообщение об обнаруженном вирусе.

1.5 Пользователь не должен изменять существующие настройки браузеров, менеджеров закачек и других программ, поскольку это изменение может повлечь снижение уровня безопасности информации на компьютере пользователя.

1.6 Пользователь должен включать DSL-соединение ТОЛЬКО на время работы в сети Интернет. В остальное время данное соединение должно быть отключено.

1.7 Пользователь самостоятельно несёт ответственность за безопасность содержания всех закачиваемых им на свой компьютер файлов из сети Интернет, а также за порчу и уничтожение файлов на своём компьютере и компьютерах рабочей локальной сети вследствие заражения их вирусной программой, находящейся в непроверенном пользователем скачанном из Интернета файле.

1.8 При обнаружении в ходе работы за компьютером подозрительных сообщений, испорченных или пропавших файлов, неработающих программ, замедлении работы компьютера и прочих нарушениях работы компьютера и оргтехники пользователь должен незамедлительно сообщить о них инженеру-программисту.

2. Обеспечение безопасности при использовании внешних носителей информации.

2.1 К внешним носителям относятся дискеты, CD и DVD диски, USB-Flash носители, подключаемые винчестеры. Поскольку данные носители также могут служить средством распространения вирусных программ, то они должны быть проверены пользователем на наличие вирусов с помощью антивирусной программы. Для этого пользователю необходимо кликнуть правой кнопкой мыши на значке проверяемого объекта в папке «Мой компьютер» и выбрать пункт «Проверить на вирусы» (рисунок 3). Если антивирусная программа не обнаружила вирусов на проверяемом носителе, то он условно считается безопасным.

2.2 Поскольку USB-Flash носители могут содержать вирусы типа autorun, невидимые для антивирусной программы, то ещё ДО подсоединения таких носителей к компьютеру пользователя и начала проверки их антивирусной программой необходимо запустить утилиту anti-autorun для удаления вирусов типа autorun, находящуюся на рабочем столе (рисунок 5), и следовать кратким инструкциям программы.

Рисунок 5. Значок утилиты Autorun

3. Резервное копирование информации пользователем.

3.1 Во избежание случайной потери файла пользователь должен делать резервные копии данного файла по мере необходимости, которая определяется пользователем исходя из степени важности данного документа, количества и частоты вносимых в файл изменений. Резервные копии данного документа могут располагаться как на жёстком диске компьютера пользователя, так и на внешних носителях. Резервному копированию

подлежат файлы Word, Excel, графические и другие виды файлов по усмотрению пользователя, за исключением файлов внутренних баз данных приложений и системных файлов. Для резервного копирования файла(-ов) необходимо выделить файл(-ы) указателем мыши, далее в контекстном меню выбранного файла(-ов) либо на панели инструментов папки выбрать пункт «Копировать», затем перейти в папку, в которую необходимо вставить файл, в контекстном меню выбранной папки либо на панели инструментов папки выбрать пункт «Вставить».

3.2 Пользователь самостоятельно несёт ответственность за безопасность содержания всех копируемых им на свой компьютер файлов, а также за порчу и уничтожение файлов на своём компьютере и компьютерах рабочей локальной сети вследствие заражения их вирусной программой, находящейся в непроверенном пользователем скопированном с внешнего носителя файле.