ИНСТРУКЦИЯ
ПО ОРГАНИЗАЦИИ АНТИВИРУСНОЙ ЗАЩИТЫ

Компьютерный вирус – это небольшая вредоносная программа, которая самостоятельно может создавать свои копии и внедрять их в программы (исполняемые файлы), документы, загрузочные сектора носителей данных, а также шифрующие файлы на жестком диске компьютера и требующие деньги за их расшифровку (Зашифрованными могут оказаться файлы *.mp3, *.doc, *.docx, *.pdf, *.jpg, *.rar и так далее...)

Антивирус на 100% не защищает компьютер от вирусов. Всегда есть доля вероятности заражения. Чаще всего виновником заражения является пользователь компьютера, который запустил зараженный файл.

Вирусы распространяются, копируя свое тело и обеспечивая его последующее исполнение: внедряя себя в исполняемый код других программ, заменяя собой другие программы, прописываясь в автозапуск и другое. Вирусом или его носителем могут быть не только программы, содержащие машинный код, но и любая информация, содержащая автоматически исполняемые команды — например, пакетные файлы и документы Microsoft Word и Excel, содержащие макросы. Кроме того, для проникновения на компьютер вирус может использовать уязвимости в популярном программном обеспечении (например, Adobe Flash, Internet Explorer, Outlook), для чего распространители внедряют его в обычные данные (картинки, тексты и т. д.) вместе с эксплоитом, использующим уязвимость.

Самый популярный путь распространения вирусов - через электронную почту. К письму прикрепляется файл, содержащий вредоносную программу, которая запускается при попытке открыть это вложение. При этом, как правило, текст письма содержит очень грамотно, психологически точно составленное сообщение, побуждающее пользователя открыть прикрепленный файл. Вот некоторые примеры (чаще они бывают на английском языке):

- "в ответ на ваш запрос высылаем..."
- "в аттаче - логи ошибок вашего сервера"
- "в аттаче – исправленный договор"
- "во вложении – счет на оплату"
- "обнаружена новая уязвимость Windows. Отправляем вам утилиту по исправлению"
- "с вашего компьютера рассылаются зараженные письма. В аттаче - утилита для лечения"

Часто такие письма содержат подпись типа "проверено антивирусом 'таким-то', вирусов не обнаружено".

Профилактика и лечение

- Не работать под привилегированными учётными записями без крайней необходимости. (Учётная запись администратора в Windows);
- Не запускать незнакомые программы из сомнительных источников;
- Стараться блокировать возможность несанкционированного изменения системных файлов;
- Отключать потенциально опасную функциональность системы (например, autorun-носителей в MS Windows, сокрытие файлов, их расширений и пр.);
- Не заходить на подозрительные сайты, обращать внимание на адрес в адресной строке обозревателя;
- Пользоваться только доверенными дистрибутивами;

- Постоянно делать резервные копии важных данных, желательно на носители, которые не стираются (например, BD-R) и иметь образ системы со всеми настройками для быстрого развёртывания;
- Не хранить важные документы на локальных компьютерах, рекомендуется использовать сетевые ресурсы Центра Интернет (выполняется регулярное резервное копирование);
- Выполнять регулярные обновления часто используемых программ, особенно тех, которые обеспечивают безопасность системы;
- Выполнять регулярные обновления операционной системы;
- Выполнять регулярные обновления антивирусной программы.

Основные признаки появления вируса в ПК:

- медленная работа компьютера;
- зависания и сбои в работе компьютера;
- изменение размеров файлов;
- уменьшение размера свободной оперативной памяти;
- значительное увеличение количества файлов на диске;
- исчезновение файлов и каталогов или искажение их содержимого;
- изменение даты и времени модификации файлов.
- И другие признаки.

В случае заражения **НЕ нужно делать:**

1. Если Ваши файлы зашифровались, то НЕ надо связываться со злоумышленниками. Это глупо. В более чем 50% случаев после «оплаты», примерно, 5000р., вы не получите НИЧЕГО. Ни денег, ни дешифратора.
2. Пытаться лечить и удалять найденные антивирусом вирусы в автоматическом режиме или самостоятельно.
3. Переустанавливать операционную систему;
4. Менять расширение у зашифрованных файлов;
5. Очищать папки с временными файлами, а также историю браузера;
6. Использовать самостоятельно без консультации со специалистом дешифраторы и прочие утилиты.

Скачать актуальную лицензионную версию антивируса можно по адресу:
http://soft.kubsu.ru/Antivirus/

Найденные антивирусной программой файлы можно переместить в «карантин» (место, указываемое антивирусной программой), а затем обратиться к специалистам.

В случае возникновения заражения компьютера вирусами, незамедлительно обращайтесь к специалистам, обслуживающим Ваш компьютер.