Памятка пользователя использованию антивирусной защиты

Типовые действия.

Авторизация. Убедиться в загрузке антивирусного программного обеспечения сразу после авторизации пользователя (и первичной, и последующих повторных, если выполнялась блокировка) и в случае его отсутствия уведомить ответственного за антивирусный контроль.

Работа с флеш-накопителем, CD-диском или любым другим отчуждаемым носителем. Перед началом работы с отчуждаемым носителем выполнить полную проверку его содержимого на вирусы, за исключением случаев, когда это сделать технически невозможно (например, Rutoken, E-Token).

Веб-серфинг (просмотр страниц сайтов и порталов через браузер). Соблюдать положение об использовании сети Интернет и электронной почты.

Получение и чтение почты. Соблюдать положение об использовании сети Интернет и электронной почты. Не переходить по ссылкам*, не распаковывать архивы (особенно запароленные) в письмах от неизвестных отправителей. Перед открытием письма, вызывающего подозрение необходимо переслать его ответственному за антивирусный контроль в организации, получить от него разрешение.

Для определения вредоносной ссылки необходимо перейти на сайт **http://virustotal.com, перейти на вкладку **URL**, вставить скопированную ссылку, нажать поиск. На безопасных ссылках будет в результате поиска будет 0 угроз, будет оформление страницы зеленым цветом и написано «**No engines detected this URL**». Во всех остальных случаях считать ссылку ***подозрительной***.

Признаки заражения компьютерным вирусом.

прекращение работы или неправильная работа ранее успешно функционировавших программ;

медленная работа компьютера;

невозможность загрузки операционной системы;

исчезновение файлов и каталогов или искажение их содержимого;

изменение даты и времени модификации файлов;

изменение размеров файлов;

неожиданное значительное увеличение количества файлов на диске;

существенное уменьшение размера свободной оперативной памяти;

вывод на экран непредусмотренных сообщений или изображений;

подача непредусмотренных звуковых сигналов;

частые зависания и сбои в работе компьютера.

При обнаружении пользователем признаков заражения объекта информатизации (далее – ОИ) вирусом

1. Отключить ОИ от компьютерной сети. В случаем с мобильным ОИ – от WiFi и от мобильной сети. В случае стационарного ОИ – отключить сетевой кабель.
2. Запустить полное сканирование на вирусы ОИ, установленным средством антивирусной защиты.
3. Сообщить об инциденте ответственному за антивирусный контроль в организации. Если средство антивирусной защиты оказалось неактивным на момент обнаружения признаков заражения ОИ, акцентировать на данном факте внимание ответственного за антивирусный контроль в организации.

Пользователю средства антивирусной защиты строго запрещено:

- изменять настройки и конфигурацию средств антивирусной защиты;
- удалять или добавлять в систему какие-либо другие средства антивирусной защиты.