Памятка по использованию электронной почты

1. Общие положения

Пользователям запрещена самостоятельная установка, настройка, обновление, деинсталляция (удаление) средств антивирусной защиты. Установка, настройка, обновление, деинсталляция средств антивирусной защиты может производиться только лицом, ответственным за обслуживание компьютерной техники.

При включении АРМ пользователь обязан проверить наличие и работоспособность средства антивирусной защиты. При отсутствии средства антивирусной защиты, его некорректной работе или обнаружении вирусного заражения пользователь незамедлительно должен сообщить об этом лицу, ответственному за обслуживание компьютерной техники.

Если в процессе работы пользователя выдается сообщение о некорректной работе или обнаружении вредоносных программ (вирусов), пользователь должен обратиться к лицу, ответственному за обслуживание компьютерной техники.

До восстановления работоспособности или установки (в случае отсутствия) средства антивирусной защиты пользователю запрещено работать в сети Интернет, подключать внешние носители информации, подключаться к сетевым файловым хранилищам, а также обрабатывать входящую почту.

2. Порядок реагирования на инциденты вирусного заражения

В случае выявления заражения АРМ (выявление признаков заражения) вредоносным ПО необходимо выключить АРМ и незамедлительно сообщить о вирусном заражении лицу, ответственному за обслуживание компьютерной техники.

3. Подключение к АРМ внешних носителей информации

При подключении к АРМ съемного носителя информации, используемого пользователем или полученного от иных лиц, пользователь обязан провести проверку носителя средствами антивирусной защиты.

В случае выявления заражения носителя необходимо незамедлительно прекратить работать с носителем (извлечь его из АРМ). Если носитель информации является штатным средством работы пользователя, его необходимо передать для проверки лицу, ответственному за обслуживание компьютерной техники; после проверки носитель разрешен к использованию. В случае если носитель информации получен от иных лиц, носитель возвращается владельцу: использование информации с данного носителя запрещено, т. к. невозможно подтвердить достоверность содержащейся информации.

4. Инструкция для сотрудника, использующего электронную почту на домене tularegion в своей деятельности.

Пользователю запрещается сообщать посторонним (третьим) лицам логины/пароли от почты, хранить их в открытом виде в доступном другим пользователям или посторонним лицам месте, например, в виде наклейки на мониторе, под клавиатурой.

При получении письма по электронной почте пользователь обязан проверить его на наличие следующих признаков, характерных для спам-письма:

а) письмо получено от неизвестного адресата;

б) в строке получателей много неизвестных адресатов либо адресаты подобраны без смысла (например, все адресаты письма имеют имя «Елена»);

в) письмо написано на иностранном языке;

г) тема и содержимое письма не совпадают;

д) письмо содержит рекламную информацию;

е) к письму приложен архив или файлы с двойным расширением (например, «резюме.босх.Бсг», «акты-zip.txt»);

ж) ярлык приложенного файла не соответствует его расширению;

з) в письме предложено перейти по ссылке для скачивания файлов либо перехода на внешний Интернет-ресурс.

Во избежание заражения пользователь не должен открывать вложения и переходить по ссылкам в письмах, имеющим признаки спам-сообщений.

Пользователь несет ответственность за заражение АРМ вследствие активации им вредоносного содержимого спам-письма.

В случае, если письмо однозначно идентифицировано пользователем как спам-сообщение, он должен переслать его на почтовый ящик spam@tularegion.ru («Нежелательная почта»).

При получении письма, в отношении которого пользователь не может определить, относится ли оно к категории спам-сообщений, необходимо переслать его для проверки на почтовый ящик servicedesk@tularegion.ru («omnitracker»), указав в качестве дополнительного адресата spam@tularegion.ru («Нежелательная почта»), с пометкой «прошу проверить на наличие вирусов».

Письма, имеющие признаки спам-письма, запрещено пересылать на другие почтовые ящики пользователей tularegion.ru.

При получении письма вследствие пересылки от других пользователей почтовой системы tularegion.ru и имеющего признаки спам- письма, необходимо выполнить действия указанные выше (Пример. На официальный почтовый ящик было получено письмо, имеющее признаки спам-письма. Данное письмо было переслано получателем на другой почтовый ящик. Для конечного получателя письмо получено от легитимного абонента и не вызывает опасения. Результат - пользователем открыто вложение спам-письма и АРМ заражено вирусом).

Сообщения, которые пользователь может однозначно определить как нежелательную почту (реклама, наличие ссылок на неизвестные ресурсы, отсутствие признаков обращения гражданина) удаляются из почтового клиента без пересылки на spam@tularegion.ru.

Сообщения, которые сотрудник не может однозначно определить как нежелательную почту, пересылается в адрес omnitracker@tularegion.ru для создания заявки на проверку письма, вложенных ссылок и приложенных файлов на признаки мошенничества и наличия вредоносного ПО.

5. Действия пользователя в случае выявления вредоносного программного обеспечения на АРМ

В случае обнаружения вредоносной программы (вируса) система антивирусной защиты автоматически предпримет действия по его обезвреживанию (блокирует, лечит зараженные файлы, удаляет не подлежащие лечению файлы, помещает зараженные файлы в карантин).

Если заражен внешний носитель информации, необходимо незамедлительно прекратить работу с ним и извлечь его из АРМ. Если носитель является штатным средством работы пользователя, необходимо обратиться в службу поддержки пользователей для детальной проверки носителя. После проверки носитель разрешен к использованию. В случае если носитель получен от иных лиц, он возвращается владельцу, и его дальнейшее использование на АРМ запрещено.

Если заражен Интернет-ресурс (далее - сайт), необходимо незамедлительно прекратить работу с ним. Если сайт является официальным ресурсом правительства

Тульской области, необходимо сообщить о факте заражения в службу поддержки пользователей.

Если заражены файлы и папки, находящиеся на сетевом файловом хранилище, необходимо незамедлительно прекратить работу с ним и сообщить о факте заражения лицу, ответственному за обслуживание компьютерной техники.

Если заражено почтовое сообщение (почтовое сообщение содержит вредоносное вложение или ссылку на сайт, являющийся источником распространения вредоносного кода), пользователь должен незамедлительно сообщить о данном почтовом сообщении лицу, ответственному за обслуживание компьютерной техники.

В случае если вредоносный код не обнаружен средством антивирусной защиты, но имеются явные признаки заражения, в частности:

а) на экран выводятся непредусмотренные сообщения, например, баннеры, блокирующие рабочий стол, информирующие вас о заражении АРМ, изображения и звуковые сигналы;

б) неожиданно открывается и закрывается лоток дисковода;

в) произвольно, без участия пользователя, запускаются какие-либо программы;

г) на экран выводятся предупреждения о попытке какой-либо из программ АРМ выйти в Интернет, или запрос на повешение прав контроля учетных записей Windows, хотя пользователь никак не инициировал такое действие;

д) исчезновение файлов и каталогов, искажение их содержимого, имен или форматов;

е) пользователю поступают жалобы, что от его имени приходят письма, которые он не отправлял, пользователь должен незамедлительно отсоединить сетевой кабель, выключить АРМ и сообщить о возможном заражении лицу, ответственному за обслуживание компьютерной техники.

В случае если вредоносный код не обнаружен, но имеются косвенные признаки заражения АРМ, в частности:

а) частые зависания и сбои в работе операционной системы и приложений, появление сообщений об ошибках;

б) проблемы при загрузке операционной системы или невозможность ее загрузки;

в) Интернет-браузер «зависает» или ведет себя неожиданным образом (например, окно программы невозможно закрыть или открывается только один Интернет-ресурс);

г) иные нетипичные для работы АРМ события,

пользователь должен самостоятельно запустить полную проверку АРМ средством антивирусной защиты. Если в результате проверки вредоносных объектов не обнаружено, пользователю рекомендуется обратиться лицу, ответственному за обслуживание компьютерной техники.