Методические рекомендации по противодействию вирусам шифровальщикам

(Разработаны в соответствии с письмом Управления ФСБ России по Ульяновской области №5-8161 от 17.12.2018 г.)

Настоящие методические рекомендации предназначены для использования при обеспечении защиты информации от воздействия вирусов шифровальщиков (ВШ) и применимы как для профилактики, так и для снижения последствий произошедшего заражения. Вирусы шифровальщики это отдельный класс вирусного программного обеспечения (ВПО) которое при заражении ПЭВМ или вычислительных систем выполняет алгоритм криптостойкого шифрования пользовательских данных, файлов, носителей информации.

Для профилактики заражения (ВШ) необходимо:

1. Выполнять требования антивирусного обеспечения, разграничения прав доступа, регламентов и рекомендаций по работе на ПЭВМ разработанных специалистами.

2. Проводить регулярное обновление антивирусных баз. Разграничить права на настройку и управление антивирусными средствами.

3. Использовать межсетевой экран (МЭ). Вести перечень разрешенных сетевых служб, разделять пользовательские сегменты по группам.

4. Проводить периодический анализ установленного ПО, прикладных программ и сервисов в целях выявления подозрительных или не являющимися необходимыми в работе. ***Для пользователей ПЭВМ УлГТУ обязательно соответствие установленного ПО с заявками поданными в центр управления лицензиями.***

5. Включить отображение расширения файлов. При запуске исполняемых файлов визуально проверять их на двойное расширение. Не запускать неизвестные, ОСОБЕННО ПОЛУЧЕННЫЕ ПО ЭЛ. ПОЧТЕ от неизвестного адресата. НИКОГДА НЕ ВЫПОЛНЯТЬ рекомендуемые действия полученные в таком эл.письме. Придерживаться правила НЕ ОТКРЫВАТЬ эл. письма от неизвестных адресов или открывать их в специальном защищенном ПО. При пересылке по эл. почте исполняемых файлов пользоваться архиваторами с паролем.

6.Запретить на пользовательских ПЭВМ (или учетных записях) запуск исполняемых файлов из временных директорий, установить пароль на загрузку на уровне BIOS. При возможности расширенного управления питанием (ACPI) установить в BIOS настройку "оставлять систему выключенной при возобновлении питания". В ОС отключить автоматическую перезагрузку при сбоях.

7. Вести контроль использования внешних носителей средствами ОС и дополнительными антивирусными средствами (АВС) с обязательной проверкой при подключении и работе с файлами. Отключить автозапуск для всех устройств и носителей информации.

8. Запретить использование общих сетевых ресурсов с автоматическими правами на запись.

9. Для предотвращения потери информации рекомендуется иметь резервные копии данных, находящиеся на периодически обновляемом изолированном от ПЭВМ ресурсе.

Признаками заражения (ВШ) могут быть:

1.Вывод на экран различных сообщений о шифровании компьютера с требованием о выкупе или предоставлении злоумышленникам каких либо данных.

2.Полная или частичная блокировка работы ПЭВМ, выдача системой различных сообщений о сбоях в системном ПО, потере загрузочных файлов, дисков .и.т.д.

3.Резкое беспричинное замедление работы ПЭВМ при отсутствии ресурсоемких задач и запущенных приложений.

4.Появление на рабочем столе или в рабочих директориях посторонних ярлыков файлов, ранее не известных программ.

5.При попытках получения доступа к файлам компьютера из под другой системы наблюдается искажение, невозможность открытия или полное отсутствие данных, либо диск является не читаемым.

В случае появления любого из вышеперечисленных признаков важно не пропустить самую раннюю стадию заражения (ВШ). С точки зрения пользователя это может выглядеть как спонтанная перезагрузка ПЭВМ или появление "синего экрана смерти". ВАЖНО не дожидаясь следующих перезагрузок выключить или обесточить компьютер и немедленно сообщить об инциденте администратору.

Если момент заражения упущен и Вы видите сообщения о каких либо действиях или требованиях ГЛАВНОЕ не проводить никаких действий с компьютером кроме немедленного обесточивания.

После заражения работа с дисками зараженной ПЭВМ должна проводиться с особой осторожностью на другом оборудовании в защищенной среде. Запрещается проводить попытки "лечения" на том-же компьютере при помощи загрузки с других носителей. После востановления данных обязательно провести проверку АВС, после чего перенести их в изолированную среду и провести проверку повторно. Зараженный диск отформатировать с обязательным удалением всех разделов и провести переустановку ОС.