Приложение №2 к распоряжению №12-р

от «23» марта 2020 г.

Действия в случае заражения рабочих вычислительных средств вирусом-шифровальщиком

**Действия администраторов.**

Рекомендованные действия для технических специалистов, ответственных за информационную безопасность, в случае, если заражение уже произошло или есть опасения, что средства вычислительной техники (далее – СВТ) заразилось вирусом-шифровальщиком:

1. Обесточить СВТ, выдернув вилку из розетки или воспользовавшись кнопкой On/Off на блоке питания. Обратите внимание, что речь идет не о кнопке включения/выключения компьютера, расположенной на лицевой стороне системного блока, а именно о тумблере блока питания (расположен сзади).
2. Обеспечить отключение зараженного устройства от сети Интернет и других сетей.

В случае, если далее предполагается обращение в правоохранительные органы по факту заражения вредоносным программным обеспечением (далее – ПО), после выполнения вышеуказанных рекомендаций должно последовать непосредственное обращение. В дальнейшем с целью снятия криминалистической копии носителей информации и проведения криминалистических экспертиз может быть принято решение об изъятии зараженных технических средств. Если обращение в правоохранительные органы не планируется или в процессе расследования оборудование не было изъято рекомендуется выполнить следующие действия:

1. Произвести загрузку операционной системы с предварительно подготовленного, защищенного от записи, носителя или использовать специальные решения антивирусных компаний (Dr.Web LiveDisk, Kaspersky Rescue Disk и др.);
2. Сделать копию зараженной системы и в дальнейшим производить все указанные действия только с копией;
3. Провести проверку копии системы с помощью антивирусного ПО;

В случае подтверждения заражения системы вирусом-шифровальщиком:

1. Если на момент обесточивания зараженной системы процесс шифрования не был закончен, скопировать нетронутые пользовательские файлы для дальнейшего использования в рабочем процессе, предварительно проверив их с помощью антивирусного ПО;
2. При наличии действующей лицензии антивирусного ПО обратиться к производителю антивируса с просьбой оказания помощи в расшифровке зашифрованной информации;
3. В случае отсутствия действующей лицензии антивирусного ПО существует вероятность расшифровки зараженной системы с помощью сообщества экспертов по информационной безопасности и открытого программного обеспечения.

Техническим специалистам, ответственным за информационною безопасность, рекомендуется провести с пользователями СВТ инструктаж на случай заражения вирусом-шифровальщиком.

**Действия пользователей**

Рекомендованные действия для пользователей в случае, если заражение уже произошло или есть опасения, что СВТ заразился вирусом-шифровальщиком:

1. Обесточить СВТ, выдернув вилку из розетки или воспользовавшись кнопкой On/Off на блоке питания. Обратите внимание, что речь идет не о кнопке включения/выключения компьютера, расположенной на лицевой стороне системного блока, а именно о тумблере блока питания (расположен сзади).

2. Обратиться к техническим специалистам, ответственными за информационную безопасность.

**Запрещенные для пользователей действия**

Ни в коем случае не стоит предпринимать следующие действия, если заражение уже произошло.

1. Осуществлять проверку и лечение компьютера с помощью антивирусного ПО;
2. Удалять или переустанавливать операционную систему;
3. Перемещать или удалять любые, в том числе незашифрованные, файлы на компьютере;
4. Изменять расширения зашифрованных файлов;
5. Использовать компьютер для выполнения любых задач;
6. Запускать утилиты дешифровки без консультации со специалистами, ответственными за информационную безопасность.