ПРИЛОЖЕНИЕ № 1

Основные меры по противодействию вирусной угрозе

1. Никогда не открывайте вложения в письмах и ссылки, содержащиеся в них, от неизвестных вам адресатов, а также подозрительные письма, пришедшие с адресов государственных органов и крупных частных организаций. В каждом таком письме должна присутствовать обратная связь, если ее нет, то существует высокая вероятность того, что письмо может содержать опасное вложение или ссылку на вирус. Лучше всего такие письма сразу удалять.

2. Настройте отображение расширения файлов. У вируса могут быть следующие расширения исполняемого файла: .exe, .bat, .cmd, .com, и т.д. Обычно вредоносные файлы распространяются в виде файлов с двойным расширением, например, «Акт сверки.xlsx.exe», и если в настройках операционной системы отключена функция отображения имени файла, то файлы такого типа будут иметь вполне легитимное наименование - «Акт сверки.xlsx». Для этого необходимо в окне «Проводник» начать кнопку «Вид» и сделать отметку в поле «Расширение имен файлов».

3. Резервируйте свою информацию. Периодически, желательно два раза в неделю, делайте резервные копии ключевой, чувствительной, важной информации на отчуждаемые носители информации, либо в защищенные разделы жесткого диска вашего компьютера.

4. Исключите использование в информационной инфраструктуре исполнительных органов государственной власти Архангельской области общедоступных облачных хранилищ, в том числе Яндекс.Диск и Диск-О.

В большинстве случаев вирус приходит вложенным в письмо электронной почты от незнакомого адресата, но возможны входящие сообщения от имени крупных государственных или частных организаций.

Электронные сообщения приходят с заголовком вида: «Судебный иск», «Акт-сверки», «Задолженность перед банком», «Проверка регистрационных данных» и прочее. В письме содержатся файлы с расширениями doc, docx, zip, xlsx, якобы подтверждающих факт, указанный в заголовке письма. При открытии таких вложения либо происходит непосредственно запуск вируса, который начинает

шифровать ваши документы, либо отображается запрос на запуск макроса, что в итоге также приводит к исполнению вируса. Также в письме, вместо вложения, может содержаться ссылка на самораспаковывающийся архив, который также содержит вредоносный код.

Если вы все же стали жертвой вируса, ни в коем случае не удаляйте инфицированное письмо и отчет антивирусной программы о его уничтожении. Без этих данных восстановление и расшифровка поврежденных файлов будет практически не возможна.