Методические рекомендации по вопросам информационной безопасности

Анализ сведений об угрозах безопасности информации происходящих с 24.02.2022, показывает, что зарубежными хакерскими группировками в отношении федеральных органов, органов исполнительной власти, а также органов местного самоуправления продолжают реализовываться компьютерные атаки, направленные на получение доступа к защищаемой информации и нарушение работы информационных систем.

Согласно поступившей из ФСТЭК России информации, одним из векторов проведения компьютерных атак в отношении информационной инфраструктуры Российской Федерации является внедрение вредоносного программного обеспечения через почтовые вложения. Нарушители используют методы социальной инженерии, отправляя пользователям электронные письма с вредоносным вложением. Эти письма приходят с заголовками вида: «Акт-сверки…», «Карточка предприятия…», «Ваша задолженность перед банком…», «Проверка регистрационных данных» и прочее. В письмах содержатся вложения с документами, якобы подтверждающими факт, указанный в заголовке письма. При открытии такого вложения происходит моментальный запуск вируса-шифровальщика, который незаметно шифрует все ваши документы, видео, изображения на всех дисках и восстановить их уже будет невозможно.

Как определить что в письме вирус? Вложения таких писем чаще всего бывают в архивах .zip, .rar, .7z, .cab. И уже внутри этих архивов находятся на первый взгляд безобидные документы. В настройках многих антивирусов по умолчанию отключена проверка архивов, поэтому необходимо проверить настройки и включить проверку архивов в антивирусном программном обеспечении.

## Как не допустить заражения? Никогда не открывать вложения в письмах от незнакомых вам людей. Всегда можно уточнить, ответив на письмо, кто отправитель, и откуда он узнал адрес вашей электронной почты, обычно ответа не последует так как владелец адреса отправления и сам может не знать что с его почты что либо отправлялось. Если же вы все равно хотите открыть вложения – обязательно проверьте расширения вложенных файлов. Если они заканчиваются на exe, .com, .js, .wbs, .hta, .bat, .cmd – ни в коем случае не открывайте их, а письмо сразу удалите.

Также в случае если к информационным ресурсам организации имеют доступ подрядные организации осуществляющие работы в рамках договора, необходимо принять следующие дополнительные меры: определить в рамках договорных отношений ответственность подрядных организаций за защиту информации при реализации удаленного доступа к информационной системе; определить перечень работников подрядных организаций, для которых предполагается удаленный доступ к информационной системе; определить перечень информации и информационных ресурсов, к которым будет предоставляться удаленный доступ работникам подрядных организаций.