ДОПОЛНИТЕЛЬНЫЕ МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ

Анализ сведений об угрозах безопасности информации, проводимый ФСТЭК России в условиях сложившейся обстановки, показывает, что зарубежными хакерскими группировками в адрес органов исполнительной власти и организаций Российской Федерации направляются фишинговые письма, содержащие вложения в виде ссылок на вредоносные файлы, которые маскируются под документы Microsoft Word (.doc, .docx) или PDF.

С целью обеспечения устойчивого функционирования рабочих мест, работающих с электронной почтой и имеющих доступ в сеть «Интернет», необходимо соблюдать следующие дополнительные меры защиты информации:

- внимательно проверять адрес отправителя, даже в случае совпадения имени с уже известным контактом;
- проверять письма, в которых содержатся призывы к действиям (например, «открой», «прочитай», «ознакомиться» и т.п.), а также с темами про финансы, банки, геополитическую обстановку или угрозы;
- не нажимать на ссылки из письма, если они заменены на слова, не наводить на них мышкой и просматривать полный адрес сайтов;
- проверять ссылки, даже если письмо получено от другого пользователя информационной системы;
- очень внимательно относиться к письмам на иностранном языке, с большим количеством получателей и орфографическими ошибками;
- использовать для работы с электронной почтой учетные записи пользователей операционной системы с минимальными возможными привилегиями;
- осуществлять проверку всех входящих писем с помощью средств антивирусной защиты с актуальными базами.

06 декабря 2023 года