С целью обеспечения устойчивого функционирования автоматизированных рабочих мест, имеющих доступ в сеть «Интернет», и предотвращения реализации угроз безопасности информации, связанных с фишингом, принять дополнительные меры защиты информации.

1. Проинформировать работников органов местного самоуправления, подведомственных им организаций о необходимости: проверки адреса отправителя, даже в случае совпадения имени с уже известным контактом; проверки писем, в которых содержатся призывы к действиям (например, «открой», «прочитай», «ознакомься»), а также с темами про финансы, банки, геополитическую обстановку или угрозы; проверки ссылок, содержащихся в электронном письме, даже если письмо получено от другого пользователя информационной системы; внимательного отношения к письмам на иностранном языке, с большим количеством получателей и орфографическими ошибками.

2. Создать отдельный электронный почтовый адрес, на который пользователи информационной системы будут присылать письма, которые могут содержать вредоносное содержание (ссылку или вложение).

3. Организовать отправку подозрительных писем, получаемых пользователями почтового сервиса, на единый (отдельный) электронный почтовый адрес для их проверки администратором безопасности. При возможности для этих целей использовать почтовую «песочницу».

4. Осуществлять проверку всех поступающих на почту вложений с использованием средств антивирусной защиты, антиспама (при наличии). Обновить базы антивирусных средств защиты до актуальных версий.

5. Использовать для работы с электронной почтой учетные записи пользователей операционной системы с минимальными возможными привилегиями.

6. Заблокировать (при возможности) получение пользователями информационной системы в электронных письмах вложений с расширениями ADE, ADP, APK, APPX, APPXBUNDLE, BAT, CAB, CHM, CMD, COM, CPL, DLL, DMG, EX, EX_, EXE, HTA, INS, ISP, ISO, JAR, JS, JSE, LIB, LNK, MDE, MSC, MSI, MSIX, MSIXBUNDLE, MSP, MST, NSH, PIF, PS1, SCR, SCT, SHB, SYS, VB, VBE, VBS, VHD, VXD, WSC, WSF, WSH