Приложение № 3

1. Заблокировать доставку писем от адреса электронной почты postin@fsteck[.]ru.

2. Проверять имя домена отправителя электронного письма в целях идентификации отправителя.

3. При получении подозрительных электронных писем от имени ФСТЭК России необходимо связаться с сотрудником ФСТЭК России и удостовериться в их легитимности.

4. Не открывать почтовые вложения форматов .7z, .rar, .zip, если заведомо не известно, что указанные вложения должны быть направлены в адрес вашего органа (организации).

5. Не открывать присланные по электронной почте файлы, использующие двойные расширения, например .pdf.exe.

6. В случае получения описанного фишингового письма от указанного почтового адреса осуществить проверку информационной инфраструктуры с использованием средств антивирусной защиты.

7. Производить проверку почтовых вложений с использованием средств антивирусной защиты:

для антивирусного средства Kaspersky Endpoint Security необходимо использовать функцию «Защита от почтовых угроз». Для того чтобы включить указанную функцию, необходимо перейти в настройки приложения и в разделе «Базовая защита» активировать функцию «Защита от почтовых угроз»;

для антивирусного средства Dr.Web Security Space необходимо использовать утилиту SpIDer Mail. Для того чтобы задействовать указанную утилиту, необходимо перейти в настройки приложения и в разделе «Компоненты защиты» выбрать и активировать утилиту SpIDer Mail.

организовать получение почтовых вложений только от известных отправителей;

не открывать и не загружать почтовые вложения писем с тематикой, не относящейся к деятельности органа (организации);

осуществлять работу с электронной почтой под учетными записями пользователей операционной системы с минимальными возможными привилегиями:

для операционных систем семейства Microsoft Windows ограничение привилегий можно осуществить через «Панель управления» - «Учетные записи пользователей» - «Управление учетными записями»;

для операционных систем семейства Linux возможно использование команд chmod, chown, chgrp для разграничения прав доступа к файлам и директориям как отдельных пользователей, так и групп пользователей;

8. Обеспечить на уровне сетевых средств защиты информации ограничение обращений к следующим адресам, используя схему доступа по «черным» или «белым» спискам:

176[.]46[.]152[.]62;

78[.]137[.]2[.]165;

212[.]15[.]49[.]30;

hxxp[:]//176[.]46[.]152[.]62[:]5858/pipanos[.]exe.

9. Осуществить настройку правил системы мониторинга событий информационной безопасности (при её наличии) путем внесения в правила корреляции событий следующих индикаторов компрометации (sha256):

f0a67866e70ad35e09d38c830432fae1af19ae7dda3b61ee357e4859285c483f;

2a9045d68491f96c0ab0777f98428872d6f233b9e64d14a4522352dc114ef2eb;

affac77085c0c26e3824efe73dd5834bd3b148659357869bf06a02a5c3e15bd0.