

Антитеррористическая комиссия в Оренбургской области

Памятка

**по действиям должностных лиц органов исполнительной государственной власти
и местного самоуправления Оренбургской области при поступлении угроз
террористического характера посредством электронных почтовых сервисов
международной информационно-коммуникационной сети Интернет**

2020 год

Общие сведения

В настоящей Памятке содержатся рекомендации по действиям должностных лиц исполнительных органов государственной власти и местного самоуправления Оренбургской области при получении по электронной почте «Microsoft Outlook», а также других интернет-ресурсов, предоставляющих услуги электронной почты (googl.com, mail.ru, yandex.ru и т. п.), информационных сообщений, которые содержат как явные признаки угрозы совершения преступлений террористического характера, так и скрытые угрозы (находящиеся во вложенных файлах).

При получении по электронной почте сообщений, содержащих признаки угрозы террористического характера, должностным лицам необходимо обеспечить условия, способствующие сохранению полученной информации с последующим обязательным информированием правоохранительных органов о получении указанных сообщений.

Раздел 1

Действия при открытом получении информации об угрозе совершения преступления террористического характера

1.1. Открытие и просмотр полученного сообщения

При открытии полученного сообщения, содержащего явные признаки угрозы совершения преступления террористического характера, без внутреннего вложения файла его содержание будет находиться в окне «Microsoft Outlook» поле «Тема».

В связи с тем, что в теме письма не могут отображаться длинные предложения, поле «Тема» может быть пустым, а текст с угрозой совершения террористического акта может содержаться в имеющемся пространстве в нижней части окна сообщения при его открытии одним кликом левой мыши, также отобразится текст письма, содержащийся в окне сообщения.

Кроме информации, содержащей угрозу совершения преступления террористического характера, в открытом окне сообщения раскрывается необходимая информация об отправителе сообщения. Также в верхней части окна сообщения отображена дата отправления сообщения, имя и электронный адрес отправителя.

1.2. Копирование и сохранение данных

Следующим шагом после открытия и просмотра полученного сообщения является копирование и сохранение информации, содержащей признаки угрозы совершения преступления террористического характера. В открытом окне сообщения отображена необходимая для копирования информация с имеющимися сведениями об отправителе сообщения и текст с содержанием угрозы террористического характера.

Для копирования полученной информации необходимо сделать скриншот (снимок экрана). На клавиатуре для этих целей предусмотрена специальная клавиша «PrintScreen» («печать экрана»), которая, как правило, находится в верхнем ряду вместе с клавишами «ScrollLock» («изначальная функция») и «Pause/Break» («приостанавливать/прерывать»), справа от клавиши «F12».

Для создания скриншота необходимо, не закрывая открытое поле полученного сообщения с содержанием угрозы совершения террористического акта, нажать на клавиатуре компьютера клавишу «PrintScreen». После нажатия указанной клавиши клавиатуры автоматически осуществляется копирование информации, содержащейся на экране компьютера, в буфер обмена, то есть копирование (фотографирование) снимка открытого поля сообщения с полученной угрозой и контактными данными отправителя сообщения. При этом внешне ничего не происходит. Рабочий стол остаётся без изменений, ничего нового не появляется, компьютер не издаёт никаких звуковых сигналов и не сопровождает произведённое действие миганием лампочек (индикаторов). Таким образом, выполнен первый шаг – копирование полученной информации.

Следующим шагом является сохранение информации с угрозой совершения террористического акта на рабочий стол компьютера пользователя. Для сохранения полученной информации необходимо создать на рабочем столе или в другом месте на жестком диске новый документ «MicrosoftWordDocument».

Далее открываем созданный документ. В появившемся окне осуществляем клик правой мыши на поле вновь созданного документа, затем последовательно подводим указатель мыши и «выбираем» одним кликом левой кнопки мыши команду «Вставить» или «выбираем» знак «Вставить» на верхней панели открытого (вновь созданного) документа «MicrosoftWordDocument».

Содержащееся в буфере обмена изображение открытого поля сообщения с полученной угрозой и контактными данными отправителя сообщения скопировалось в окно созданного документа «MicrosoftWordDocument».

По завершению вышеуказанных действий сохраняем размещённый скриншот снимка экрана в созданном документе «MicrosoftWordDocument». Для этого необходимо нажать знак «Сохранить» на верхней панели документа «MicrosoftWordDocument» или закрыть документ с подтверждением сохранения при открытии активного диалогового окна.

Снимок сообщения с полученной угрозой и контактными данными отправителя сообщения успешно сохранён. Теперь этот снимок (фотография, скриншот) находится в виде файла в компьютере пользователя.

Раздел 2

Действия при получении информации об угрозе совершения преступления террористического характера, находящейся во вложенном файле письма, поступившего по электронной почте «MicrosoftOutlook»

При получении письма по электронной почте «MicrosoftOutlook» часто прилагается какой-либо файл (документ, фотографии, видео и т.п.). Приложенный к письму файл называется вложением. Письма, содержащие вложение, подразделяются на 2 вида:

2.1. В письме, содержащем вложение, явные признаки угрозы террористического характера могут отображаться в поле «Тема» или в пространстве нижней части окна сообщения.

2.2. В письме, содержащем вложение, могут отсутствовать в поле «Тема» или в пространстве нижней части окна сообщения явные признаки угрозы совершения террористического акта.

Во всех вышеприведённых примерах получения по электронной почте писем с вложениями (пункты 2.1 и 2.2 настоящего раздела) открываем прилагаемое к письму вложение. При обнаружении (подтверждении) признаков угрозы совершения террористического акта во вложении письма необходимо:

– выполнить аналогичные действия по сохранению электронного адреса и контактных данных отправителя письма в соответствии с разделом 1;

– сохранить прилагаемое к письму вложение (документ, аудиофайл, фотографию, видео и т.п.) на рабочий стол монитора или другое место на жестком диске компьютера.

Для того, чтобы сохранить прилагаемое к письму вложение необходимо:

1. Выполнить двойной клик левой кнопкой мыши на поступившее по электронной почте письмо, затем кликнуть правой кнопкой мыши на прилагаемый файл и выбрать команду «Сохранить как».

В открывшемся окне «Сохранение документа» слева отображён список папок, в которые компьютер предлагает сохранить необходимый документ (файл). По умолчанию документ будет сохранён в папку «Мои документы», если не выбрать другую папку. Кликом левой кнопки мыши «выбираем» необходимую папку или «Рабочий стол». В окне «Имя файла» подсвечено название, которое компьютер присваивает вашему документу. Можно заменить это название своим. После чего нажать команду «Сохранить».

Обратите внимание! Если вы не меняли название документа и папку назначения, то обязательно запомните, куда сохранили документ.

2. Можно сохранить файл другим способом: выполнить клик правой кнопкой мыши на прилагаемый файл и выбрать команду «Копировать», затем свернуть окно электронной почты, выполнить клик правой кнопкой мыши на свободном месте рабочего стола вашего компьютера и выбрать команду «Вставить».

Прилагаемое к письму вложение успешно сохранено на рабочий стол монитора компьютера. Учитывая, что на рабочем столе сохранён ещё и снимок сообщения с полученной угрозой и контактными данными отправителя сообщения, целесообразно создать отдельную папку, присвоить ей соответствующее название и переместить в неё оба файла.

Таким образом, завершены все действия по копированию и сохранению информации с угрозами террористического характера, поступившей по электронной почте «MicrosoftOutlook». Сами письма после прочтения останутся в папке «Входящие» электронной почты «MicrosoftOutlook».

Необходимо отметить, что присланные по электронной почте программы, файлы и/или ссылки могут быть вредоносными и подвергать компьютер заражению, в связи с чем, после получения информации, содержащей угрозы террористического характера, не рекомендуется выполнять какие-либо действия с поступившими материалами, кроме их копирования и сохранения.

Раздел 3

Действия при получении информации об угрозе совершения преступления террористического характера, поступившей по электронной почте из иных электронных почтовых сервисов

международной информационно-коммуникационной сети Интернет (google.com, mail.ru, yandex.ru, list.ru, hotmail.com, bk.ru и т. п.)

Как правило, должностными лицами органов власти, организаций и учреждений области в целях обмена электронной корреспонденцией используется электронная почта «MicrosoftOutlook». В разделах 1 и 2 настоящей Памятки изложен порядок действий должностных лиц органов власти, организаций и учреждений автономного округа при поступлении угроз террористического характера применительно к электронной почте «MicrosoftOutlook».

Тем не менее, у различных пользователей могут быть разные «почтовые ящики» (электронная почта), в зависимости от того, на каком ресурсе, предоставляющем услуги электронной почты, создана учетная запись электронной почты (аккаунт). Это может быть google.com, mail.ru, yandex.ru, list.ru, hotmail.com, bk.ru и т. п.

У некоторых пользователей имеется несколько «почтовых ящиков», предоставленных разными почтовыми интернет-сервисами. Но принцип работы во всех «электронных ящиках» примерно одинаковый. Соответственно, независимо от вида электронной почты, на любой компьютер пользователя (должностного лица) может поступить информация с угрозой террористического характера. Таким образом, в случае получения сообщений с угрозами на любой из «почтовых ящиков», учитывая схожесть работы различных электронных «почтовых ящиков», должностным лицам органов власти, организаций и учреждений области необходимо выполнить порядок действий, предусмотренный разделами 1, 2 настоящей Памятки. При открытии на рабочем компьютере других «почтовых ящиков» (майл, яндекс и т. п.) скриншот (снимок экрана) производится аналогично с помощью клавиши «PrintScreen» (принтскрин). В случае возникновения затруднительной ситуации по копированию и сохранению сообщений, содержащих угрозы террористического характера, пользователям персональных компьютеров необходимо обратиться в службу технической поддержки (к техническому работнику) органа власти (организации, учреждения), обслуживающую работу офисной техники и информационно-телекоммуникационной сети Интернет, обеспечив при этом наименьшую осведомлённость посторонних лиц о поступлении информации об угрозе террористического характера.

Раздел 4

Последовательность действий должностных лиц органов власти, организаций и учреждений при получении информации об угрозе совершения преступления террористического характера, поступившей посредством электронных почтовых сервисов международной информационно-коммуникационной сети Интернет.

4.1. При получении по электронной почте сообщений, содержащих угрозы террористического характера, должностным лицам органов власти, организаций и учреждений необходимо:

– проинформировать непосредственного руководителя (начальника) органа власти, организации (учреждения);

- немедленно по телефону проинформировать о поступлении угрозы совершения террористического акта территориальные подразделения МВД России, ФСБ России;
- обеспечить условия, способствующие сохранению полученной информации посредством выполнения порядка действий, предусмотренных настоящей Памяткой;
- принять меры, ограничивающие доступ посторонних лиц к рабочему месту и работу с электронной почтой, на которую поступило сообщение с угрозой террористического характера;
- по возможности распечатать сохранённые материалы с угрозой террористического характера и направить посредством факсимильной связи в дежурную часть территориального подразделения ФСБ и МВД России с сопроводительным письмом, в котором должны быть указаны конкретные сведения о поступившем сообщении (вид ресурса сети интернет, предоставляющего услуги электронной почты; от кого и когда поступило сообщение; количество поступивших сообщений; вид поступившего сообщения (документ, аудиофайл, фотографии, видео и т.п.), а также содержание поступившей угрозы и другие данные;
- по прибытии сотрудников правоохранительных органов (сотрудников МВД, ФСБ) подробно ответить на их вопросы и обеспечить им доступ к рабочему месту и электронной почте вашего компьютера.

4.2. При получении по электронной почте сообщений, содержащих угрозы террористического характера, должностным лицам органов власти, организаций и учреждений ЗАПРЕЩАЕТСЯ:

- перемещать из папки «Входящие» и (или) удалять поступившие по электронной почте сообщения об угрозе теракта;
- расширять круг лиц, ознакомившихся с содержанием поступившего сообщения;
- отвечать на поступившее сообщение отправителю (адресату) письма с угрозой террористического характера;
- открывать (запускать, устанавливать) программы и/или ссылки, поступившие одновременно (в том числе во вложении к письму) с информацией об угрозе террористического характера.

**НЕ БУДЬТЕ РАВНОДУШНЫМИ,
ВАШИ СВОЕВРЕМЕННЫЕ ДЕЙСТВИЯ
МОГУТ ПОМОЧЬ ПРЕДОТВРАТИТЬ
ТЕРРОРИСТИЧЕСКИЙ АКТ
И СОХРАНИТЬ ЖИЗНИ ОКРУЖАЮЩИХ**