ИНСТРУКЦИЯпо действиям должностных лиц органов государственной властии местного самоуправления, организаций и учреждений при поступлении угроз террористического характерапосредством электронных почтовых сервисов международнойинформационно-коммуникационной сети Интернет

Общие сведения

Инструкция по действиям должностных лиц органов государственной власти и местного самоуправления, организаций и учреждений при поступлении угроз террористического характера посредством электронных почтовых сервисов международной информационно-коммуникационной сети Интернет (далее – Инструкция).

В настоящей Инструкции содержатся рекомендации по действиям должностных лиц органов государственной власти и местного самоуправления, организаций и учреждений при получении по электронной почте «MicrosoftOutlook», а также из других интернет-ресурсов, предоставляющих услуги электронной почты (google.com, mail.ru, yandex.ru, list.ru, hotmail.com, bk.ru и т.п.), информационных сообщений, которые содержат как явные признаки угрозы совершения преступления 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. Открытие и просмотр полученного сообщения.

Вид открытого сообщения без внутреннего вложения файла, содержащего явные признаки угрозы совершения преступления террористического характера, в окне «MicrosoftOutlook» поле «Тема» (рис. 1).

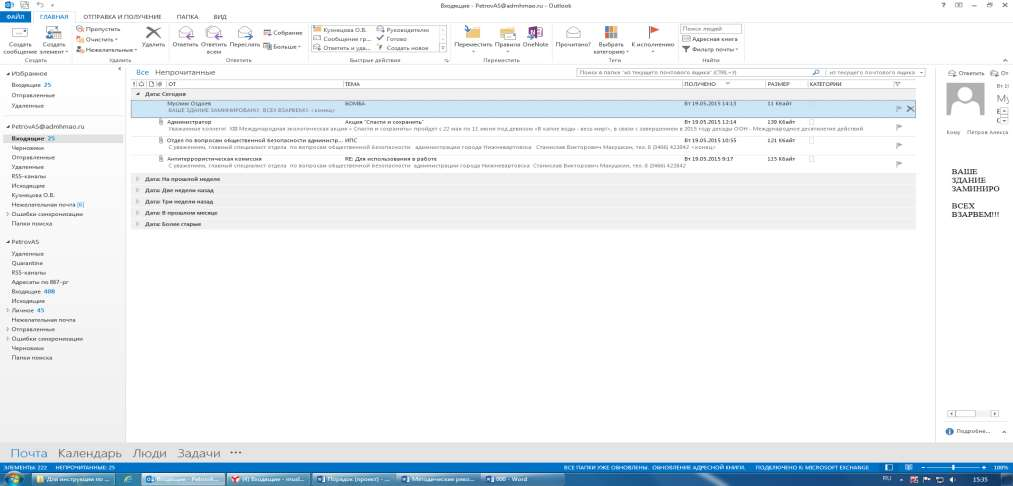


Рис. 1. – Вид сообщения

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 (рис. 2).

ВАШЕ ЗДАНИЕ ЗАМИНИРОВАН!!!

ВСЕХ ВЗАРВЕМ!!!

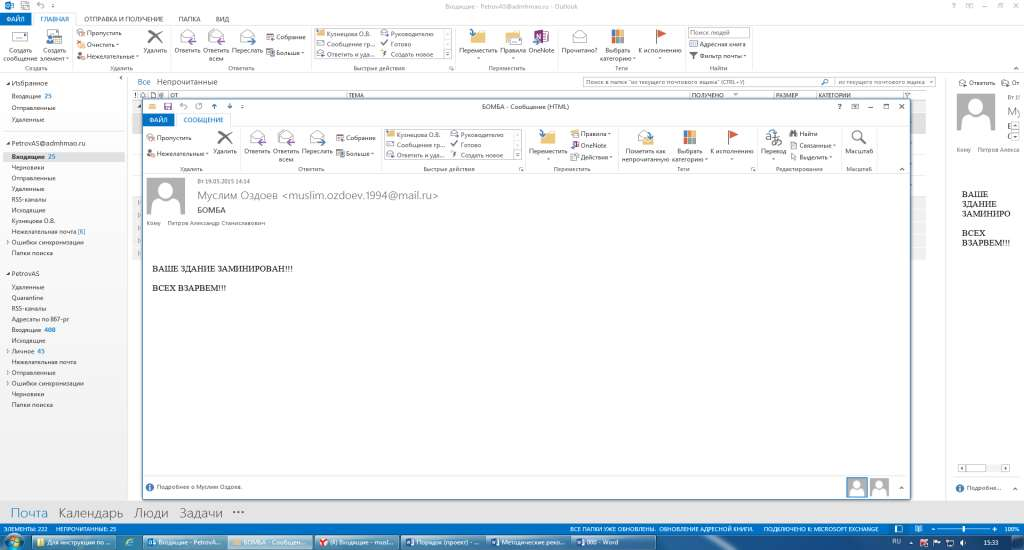


Рис. 2. – Сообщение в открытом окне

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 (рис. 3).

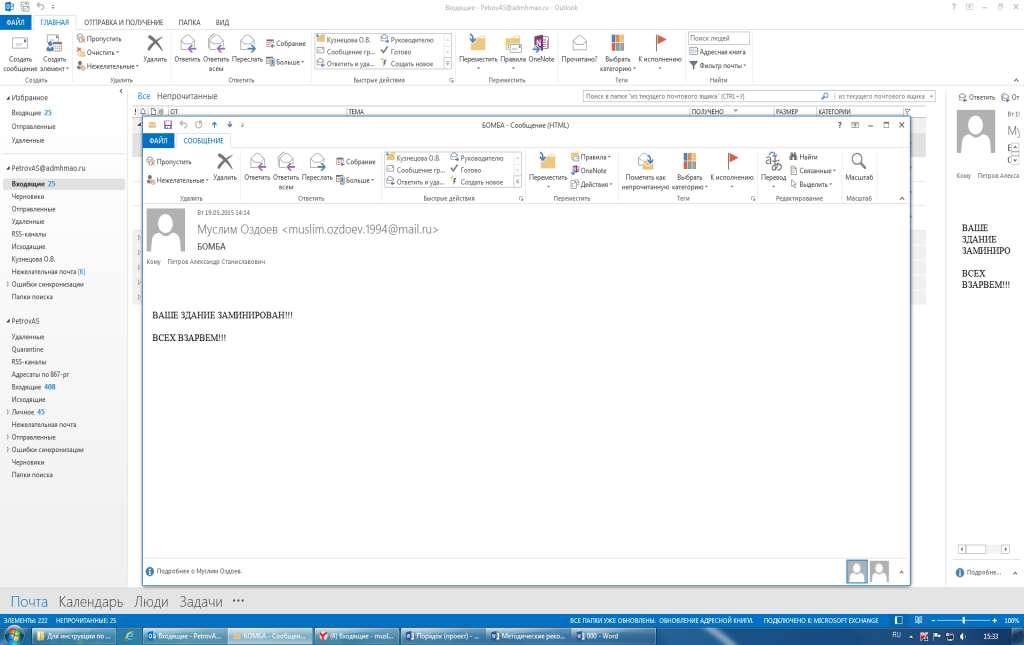


Рис. 3. – Дата, имя и электронный адрес отправителя полученного сообщения

**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»** (рис. 4).



Рис. 4. – Расположение клавиши «PrintScreen» на клавиатуре компьютера

Содержащееся в буфере обмена изображение открытого поля сообщения с полученной угрозой и контактными данными отправителя сообщения скопировалось в окно созданного документа «MicrosoftWordDocument». Прилагаемое к письму вложение необходимо сохранить на рабочий стол монитора компьютера. 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 2**

**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 в целях обмена электронной корреспонденцией используется электронная почта «MicrosoftOutlook». В разделах 1 и 2 настоящей Инструкции изложен порядок действий должностных лиц органов власти, организаций и учреждений 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 необходимо выполнить порядок действий, предусмотренный разделами 1, 2 настоящей Инструкции. 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), обслуживающих работу офисной техники и информационно-телекоммуникационной сети Интернет,

обеспечив при этом наименьшую осведомлённость посторонних лиц о поступлении информации об угрозе террористического характера.

**Раздел 3**

**Последовательность действий должностных лиц органов власти, организаций и учреждений автономного округа при получении**

**информации об угрозе совершения преступления террористического характера, поступившей посредством электронных почтовых сервисов международной информационно-коммуникационной сети Интернет**

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

- немедленно по телефону проинформировать о поступлении угрозы совершения террористического акта территориальные подразделения МВД России, Оперативный штаб в муниципальном образовании, Аппарат Антитеррористической комиссии;

- обеспечить условия, способствующие сохранению полученной информации посредством выполнения порядка действий, предусмотренных настоящей Инструкцией;

- проинформировать непосредственного руководителя (начальника) органа власти, организации (учреждения).