



**МКУ «Управление по делам гражданской обороны и  
чрезвычайным ситуациям Суздальского района»**

## **ПАМЯТКА**

**по действиям должностных лиц органов местного самоуправления,  
организаций и учреждений Суздальского района  
при поступлении угроз террористического характера  
посредством электронных почтовых сервисов международной  
информационно-коммуникационной сети Интернет**

## Раздел 1

### Действия при открытом получении информации об угрозе совершения преступления террористического характера

#### 1.1. Открытие и просмотр полученного сообщения

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

#### 1.1. Открытие и просмотр полученного сообщения

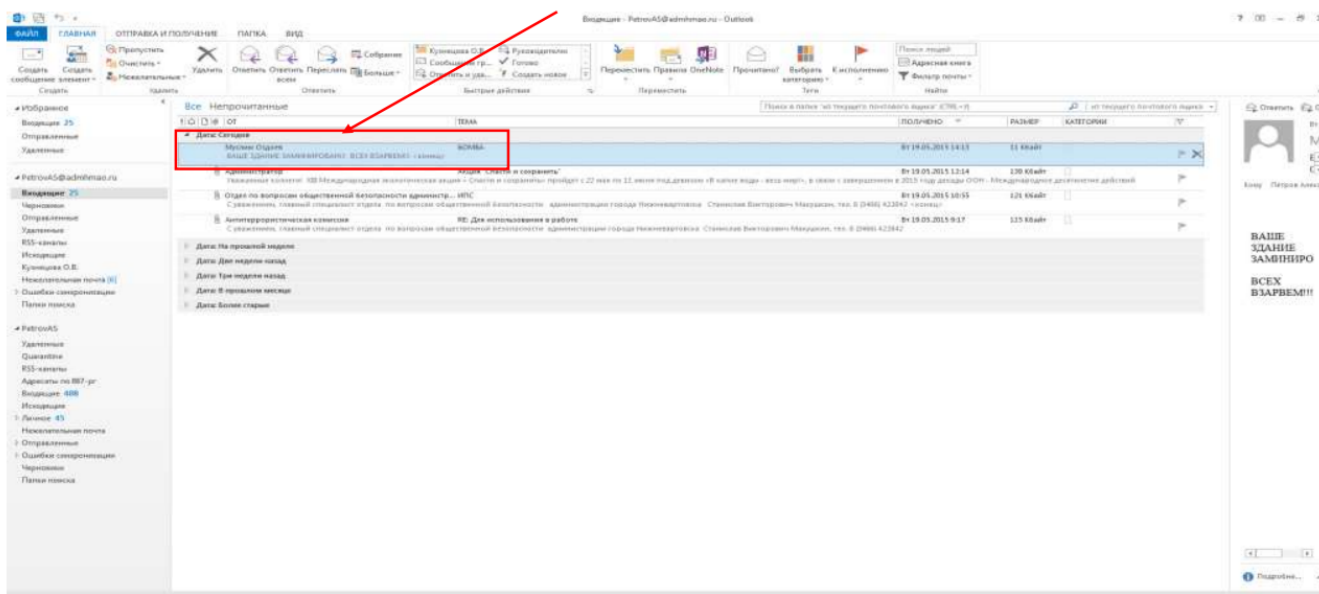


Рис. 1. – Вид сообщения

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).

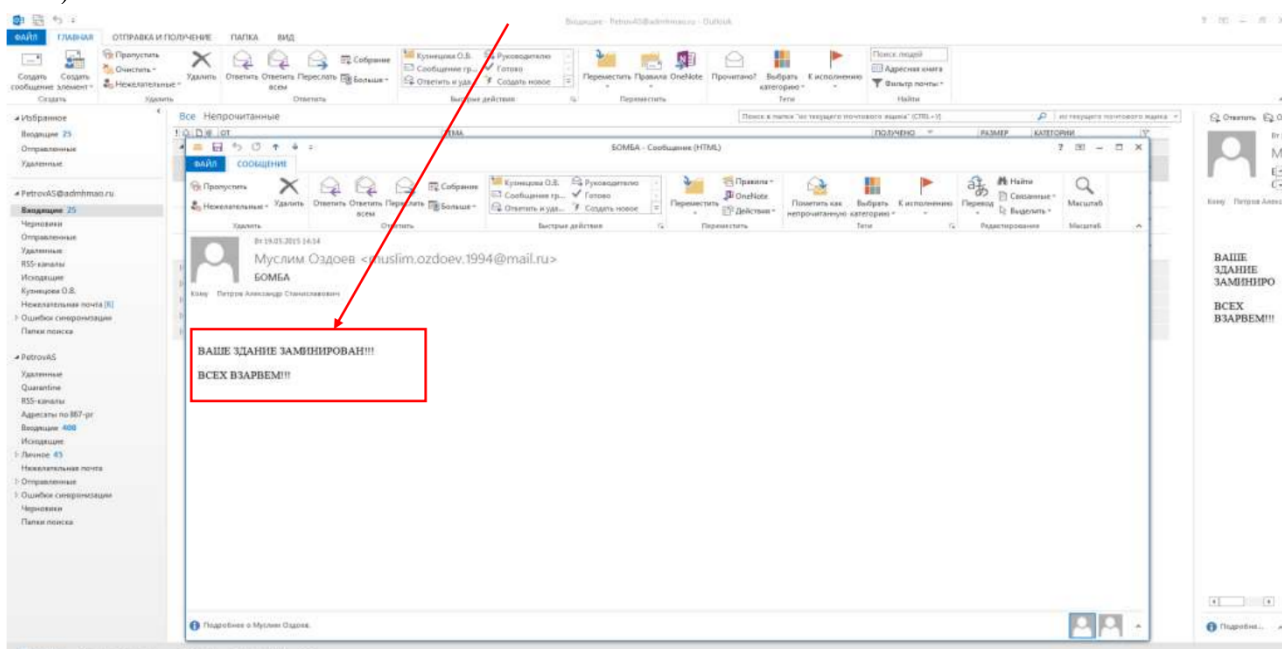


Рис. 2. – Сообщение в открытом окне

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 (рис. 3), имя и электронный адрес отправителя (рис. 4).

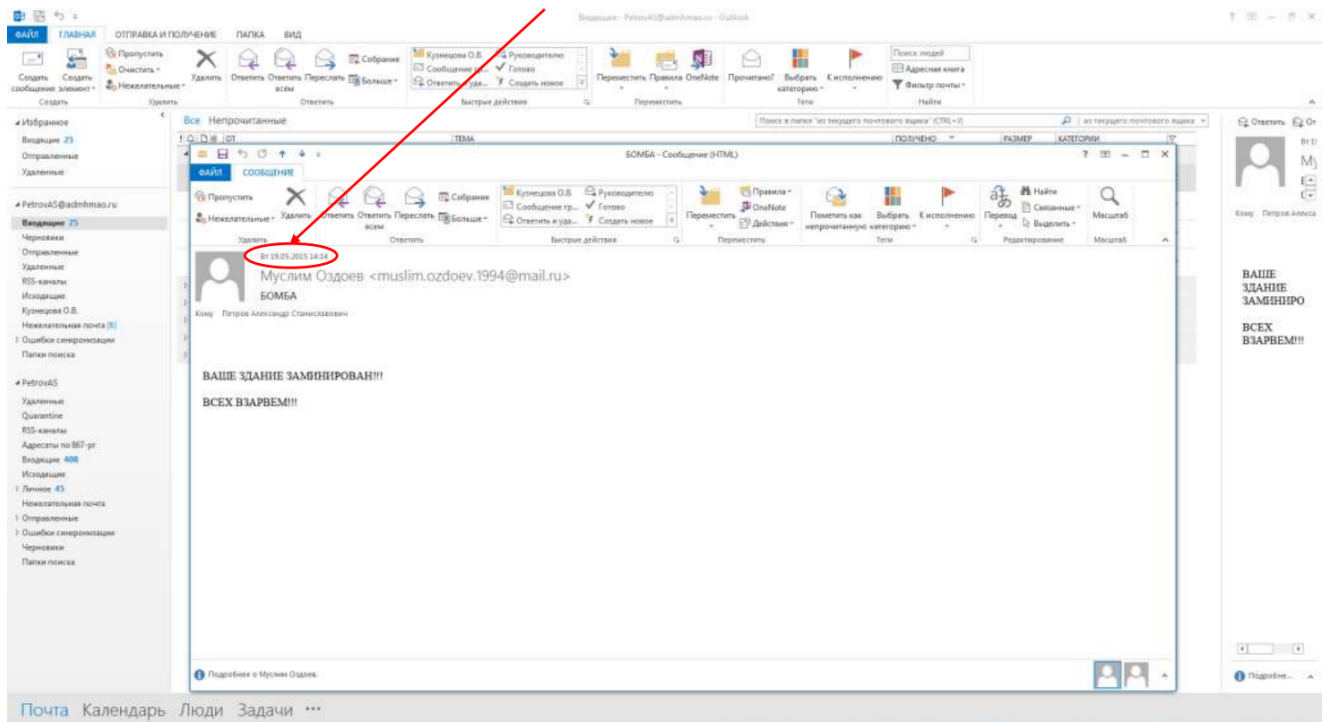


Рис. 3. – Дата полученного сообщения

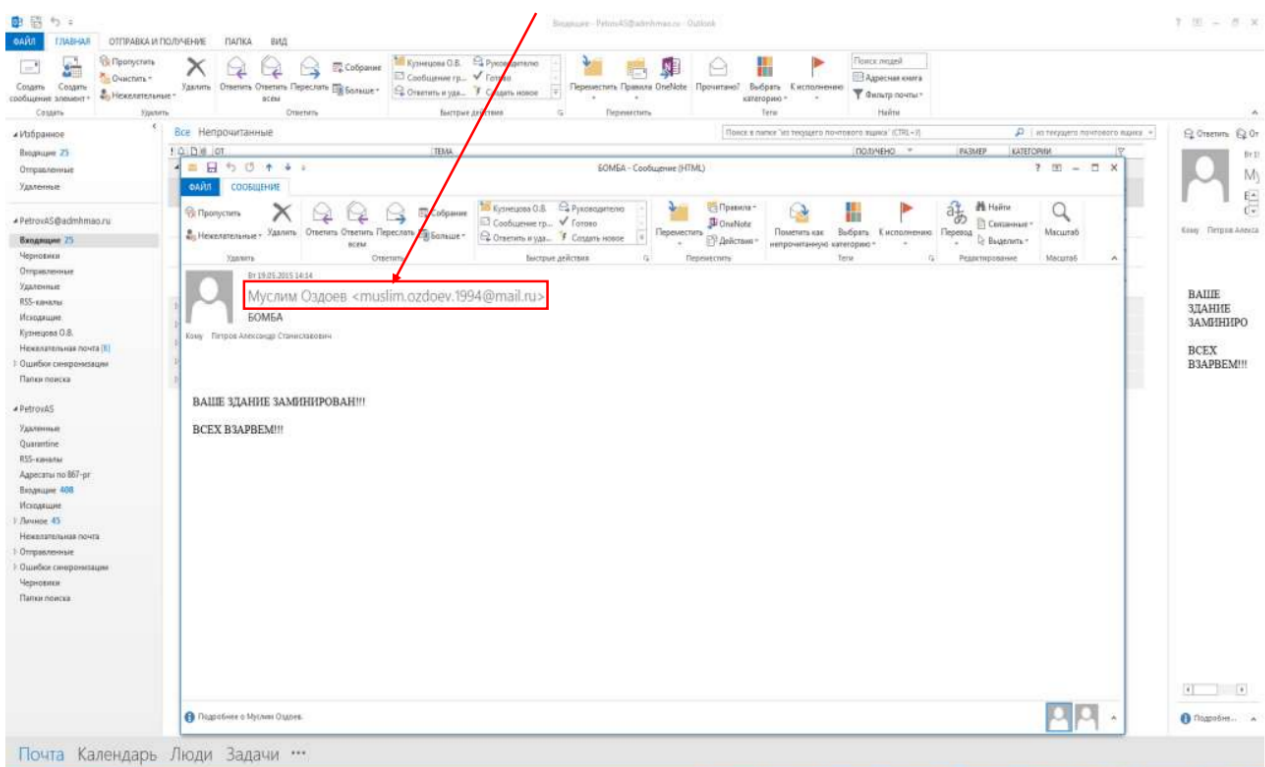


Рис. 4. – Имя и электронный адрес отправителя сообщения

## 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 (рис. 5).

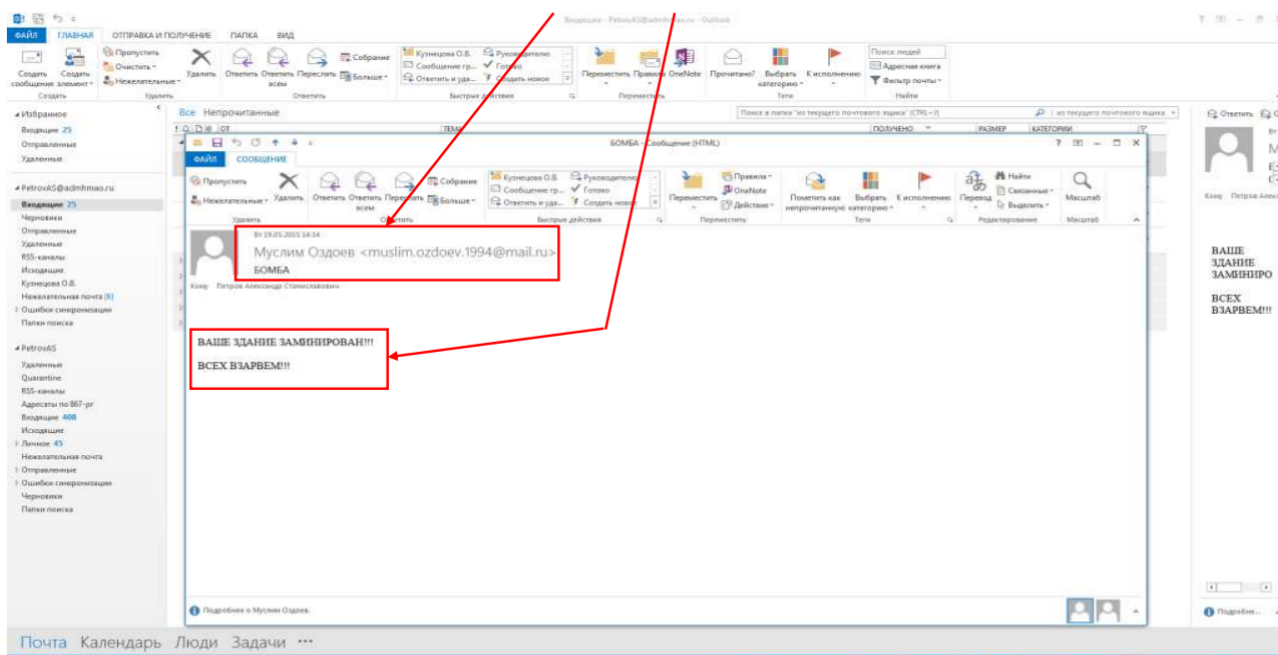


Рис. 5. – Информация в открытом окне полученного сообщения

Для копирования полученной информации необходимо сделать скриншот (снимок экрана). На клавиатуре для этих целей предусмотрена специальная клавиша «PrintScreen» («печать экрана») (рис. 6).

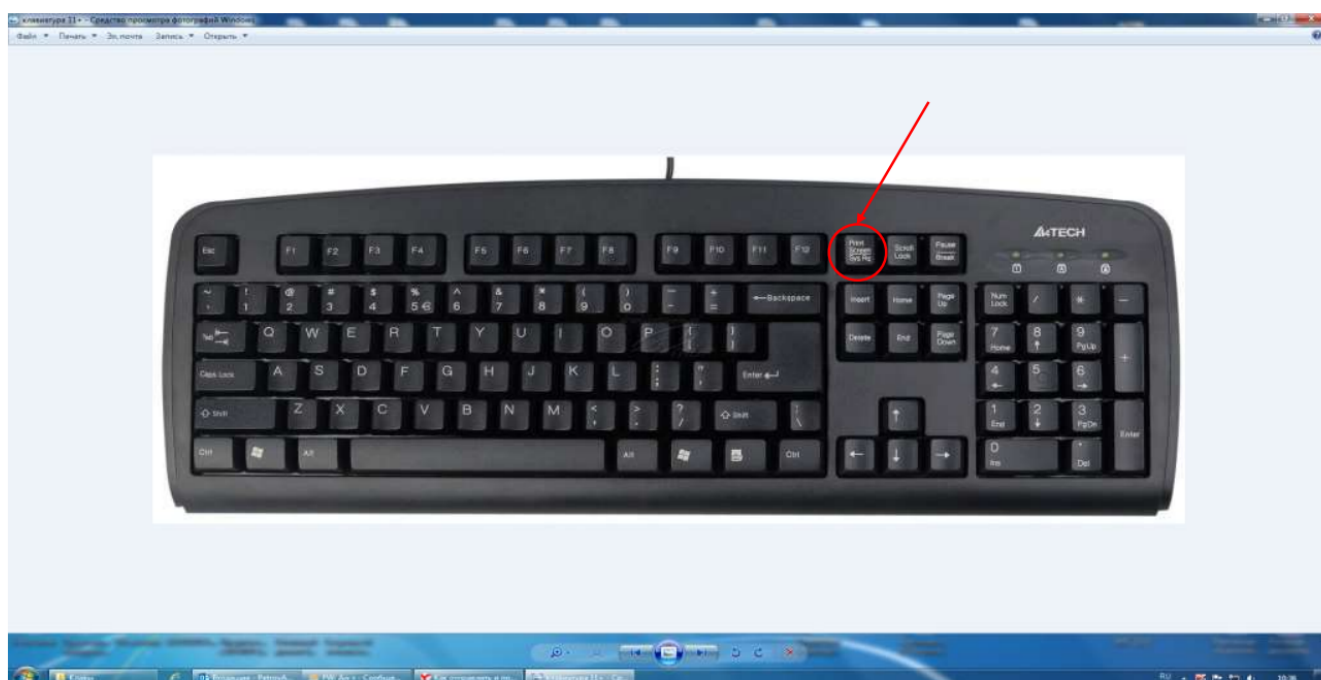


Рис. 6. – Расположение клавиши «PrintScreen» на клавиатуре компьютера

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. 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» (рис. 7).

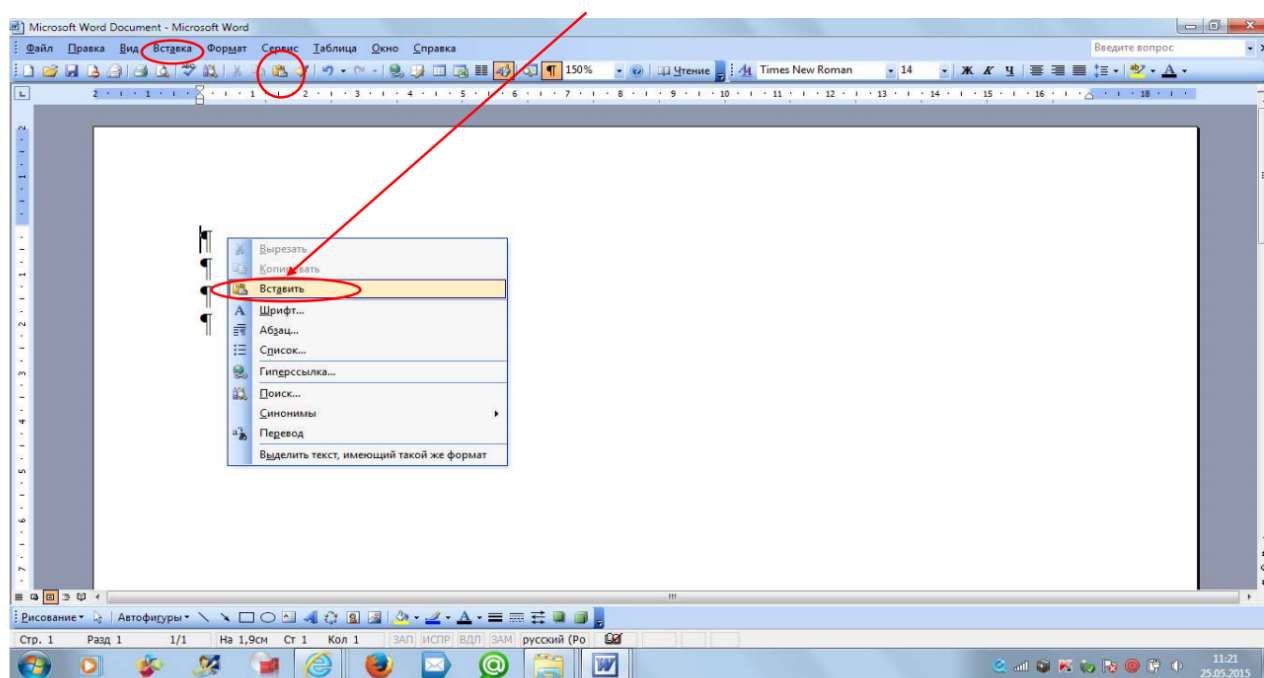


Рис. 7. – Добавление скриншота в созданный документ «MicrosoftWordDocument»

Содержащееся в буфере обмена изображение открытого поля сообщения с полученной угрозой и контактными данными отправителя сообщения скопировалось в окно созданного документа «MicrosoftWordDocument» (рис. 8).

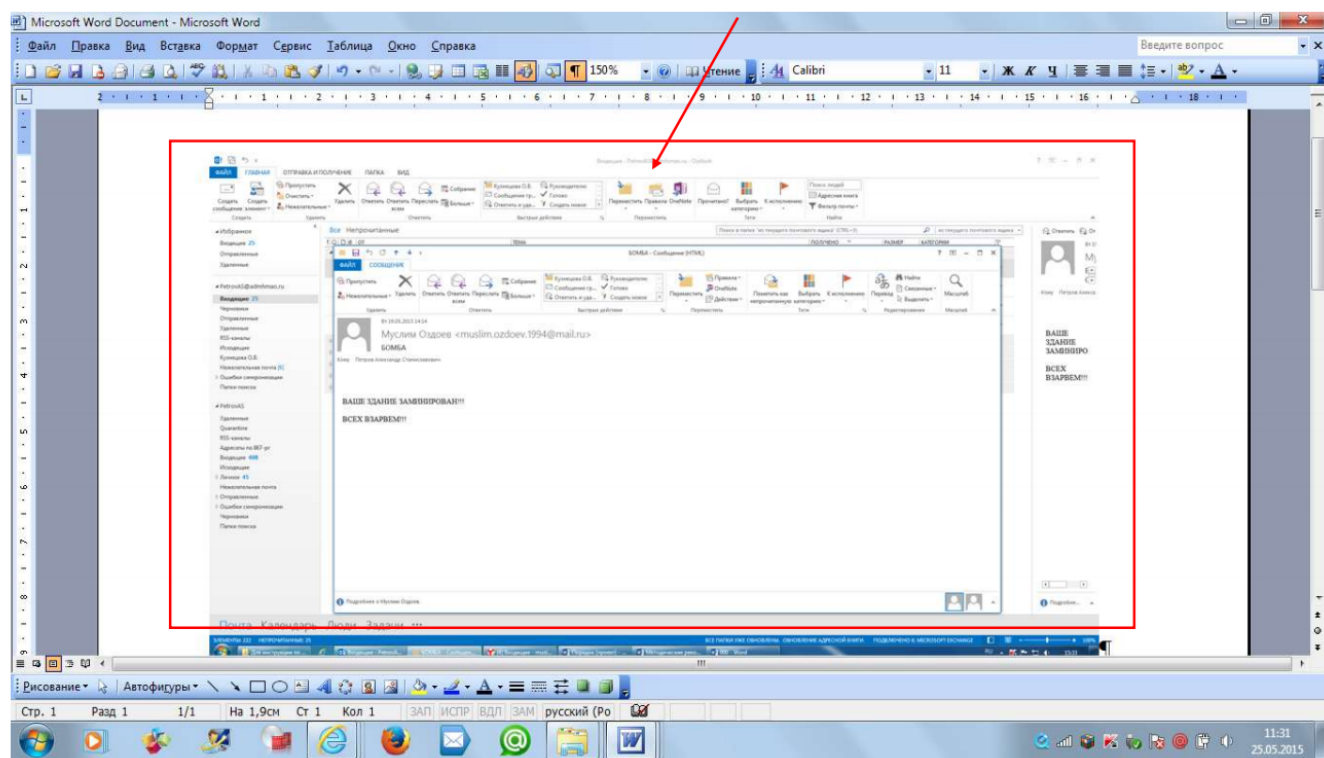


Рис. 8. – Размещение скриншота в созданном документе «MicrosoftWordDocument»

По завершению вышеуказанных действий сохраняем размещённый скриншот снимка экрана в созданном документе «MicrosoftWordDocument». Затем выводим файл на печать.

## Раздел 2

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

Зачастую при получении письма по электронной почте «MicrosoftOutlook» прилагается какой-либо файл (документ, фотографии, ссылки, программы, видео и т.п.). Приложенный к письму файл называется вложением. 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. Открывать вложения и выполнять какие-либо действия с поступившими материалами кроме их копирования и сохранения не рекомендуется.

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 (рис. 3-8).

## 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 местного самоуправления, организаций и учреждений Суздальского района в целях обмена электронной корреспонденцией используется



электронная почта «MicrosoftOutlook» или другие средства электронной почтовой связи. В разделах 1 и 2 настоящей Памятки изложен порядок действий должностных лиц органов местного самоуправления, организаций и учреждений Суздальского района 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 местного самоуправления, организаций и учреждений Суздальского района 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 местного самоуправления (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 местного самоуправления, организаций и учреждений Суздальского района 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 местного самоуправления, организаций и учреждений Суздальского района необходимо:

- проинформировать Главу органа местного самоуправления или непосредственного руководителя организации (учреждения);
- обеспечить незамедлительную пересылку сообщений, содержащих угрозы террористического характера, на специальную электронную почту антитеррористической комиссии Владимирской области [ugrozata@vinfo.ru](mailto:ugrozata@vinfo.ru). Вместе с тем, УФСБ России по Владимирской области рекомендуется установить настройку фильтрации сообщений для обеспечения автоматической пересылки сообщений с угрозами терроризма на указанный почтовый ящик;
- немедленно по телефону проинформировать о поступлении угрозы совершения террористического акта ОМВД России по Суздальскому району по телефону 02 / 102 / 2-12-35;
- немедленно по телефону проинформировать о поступлении угрозы совершения террористического акта отделение в г. Суздаль УФСБ России по Владимирской области по телефону 2-13-54;
- выполнить действия, предусмотренные разделом 1-3 настоящей Памятки, направить распечатанный файл с полученной информацией посредством факсимильной связью в отделение

в г. Суздаль УФСБ России по Владимирской области (факс 2-13-54) и в ОМВД России по Суздальскому району (факс 2-19-28);

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

- по прибытию сотрудников правоохранительных органов (сотрудников ОМВД, УФСБ) 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 местного самоуправления, организаций и учреждений Суздальского района **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!!!**