

МИНИСТЕРСТВО СЕЛЬСКОГО ХОЗЯЙСТВА
РОССИЙСКОЙ ФЕДЕРАЦИИ

ФГБОУ ВО БРЯНСКИЙ ГАУ

АГЕЕНКО Л.В., КОЗАРЕЗ И.В.

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ
по противодействию идеологии экстремизма
и действиям персонала и обучающихся
ФГБОУ ВО Брянский ГАУ
при возникновении угрозы совершения
террористического акта

Брянская область, 2022

УДК 323.28:378(07)

ББК 66.4:77.58

А 23

Агеенко Л.В., Козарез И.В. Методические рекомендации по противодействию идеологии экстремизма и действиям персонала и обучающихся ФГБОУ ВО Брянский ГАУ при возникновении угрозы совершения террористического акта./ Л.В.Агеенко, И.В. Козарез – Брянск: Издательство Брянского государственного аграрного университета, 2022. – 44 с.

Методические рекомендации разработаны на основании Закона Российской Федерации «О безопасности» 05.03.92 № 2446-1, Федерального закона «О борьбе с терроризмом» 25.07.9X г. №130-ФЗ, Федерального закона РФ «О гражданской обороне» 12.02.98 № 28-ФЗ, Федерального закона РФ «О защите населения и территории от чрезвычайных ситуаций природного и техногенного характера» 21.12.94 г. №68-ФЗ, приказа Министерства образования и науки РФ «О комплексе мер по противодействию терроризму в сфере образования и науки» от 04.06.2008г. № 170, письма Министерства просвещения РФ от 29.08.2019 г. № 06-920 «Методические рекомендации по планированию и информационному сопровождению мероприятий Комплексного плана противодействия идеологии терроризма в Российской Федерации на 2019-2023 годы в субъектах Российской Федерации».

Методические рекомендации предназначены для обучающихся, руководителей, специалистов и персонала университета.

© Брянская ГАУ, 2022
© Агеенко Л.В., 2022

Оглавление

1 Действия персонала и охраны объектов ФГБОУ ВО Брянский ГАУ	
по действиям при нападении вооружённых преступников	4
2 Действия при обнаружении взрывного устройства	
в почтовом отправлении	7
3 Действия при обнаружении подозрительных предметов, вещей	8
4 Алгоритм действия работников при получении подозрительных	
почтовых отправлений	10
5 Порядок действий при получении сообщений, содержащих угрозы	12
6 Порядок действий персонала и обучающихся по действиям	
при захвате заложников	14
7 Правила обращения с анонимными материалами, содержащими угрозы	
террористического характера	16
8 Памятка по действиям сотрудников ФГБОУ ВО Брянский ГАУ при	
поступлении угроз террористического характера посредством электронных	
почтовых сервисов международной информационно-коммуникационной сети	
Интернет	16
ПАМЯТКА	17
Общие сведения	18
Раздел 1	
Действия при открытом получении информации об угрозе совершения	
преступления террористического характера	19
Раздел 2	
Действия при получении информации об угрозе совершения преступления	
террористического характера, находящейся во вложенном файле письма,	
поступившего по электронной почте «MicrosoftOutlook»	30
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.)	42
Раздел 4	
Последовательность действий сотрудников организаций при получении	
информации об угрозе совершения преступления террористического характера,	
поступившей посредством электронных почтовых сервисов международной	
информационно-коммуникационной сети Интернет	43

1 Действия персонала и охраны объектов ФГБОУ ВО Брянский ГАУ по действиям при нападении вооружённых преступников

Не нужно вступать в конфликт с вооружённым преступником и пытаться его обезвредить. Главная задача - спасти жизнь детей. Не допускать паники, истерики и спешки. Успокоить детей.

Если слышны выстрелы или крики в другой части университета:

1. Оценить обстановку. Определить, что происходит.

2. Немедленно сообщить о случившемся руководителю образовательной организации (лицу, его замещающему), по его указанию или самостоятельно в службы экстренного реагирования (в полицию тел. 02 (с мобильного телефона – 102), в ФСБ тел. 8-(4832) 64-91-21 или в единую дежурно-диспетчерскую службу тел. 112).

3. В дальнейшем действовать по указанию руководителя или самостоятельно исходя из обстановки.

4. Обеспечить выполнение всех рекомендаций и требований прибывших сотрудников служб экстренного реагирования.

При возможности безопасно покинуть помещение:

1. Организовать экстренную эвакуацию через ближайшие выходы (запасные выходы). В отдельных случаях эвакуация может быть организована через окна первых этажей здания. Не тратить время на разговоры, сбор вещей и одевание. Место для сбора после эвакуации должно быть выбрано на достаточном удалении от учебного корпуса и (или) общежития.

2. Организовать проверку наличия студентов и сотрудников. Сообщить информацию об их наличии руководству (при возможности), а также прибывшим сотрудникам правоохранительных органов и спасательных подразделений.

3. Организовать взаимодействие с правоохранительными органами по вопросам доведения до них информации о происшествии и принятия мер по обеспечению безопасности студентов и сотрудников в районе эвакуации.

При невозможности безопасно покинуть помещение:

1. Закрыть помещение на ключ. При отсутствии ключа от помещения – **забаррикадировать дверь** (партой, шкафом, стульями и т.п.).

2. Выключить свет в помещении (тёмное время суток).

3. Организовать тишину и выключение звука на мобильных устройствах, чтобы не привлекать внимание преступника.

4. По возможности спрятать студентов.

Если преступник близко и нет возможности успеть убежать или спрятаться:

1. Не пытаться договориться с преступником. В большинстве случаев это бесполезно и опасно. Не заговаривать с ним, не обращаться к нему первым, не смотреть ему в глаза. Стараться вообще не смотреть ему в лицо и не привлекать к себе внимание.

2. **Не делать никаких резких движений.** Не надо спорить. Выполнять все требования. Оценить два пункта: какое оружие в руках у нападающего и не преграждает ли он путь к выходу.

Если у нападающего огнестрельное оружие рекомендуется:

1. **Найти безопасное место**, постараться закрыть их от случайных пуль.
2. **Держаться как можно ниже** (присесть или лечь на пол). При беспорядочной стрельбе уменьшается вероятность оказаться на линии огня.
3. **Держать нападающего в поле зрения.**
4. **В крайнем случае, попытаться отвлечь нападающего на себя и дать возможность спастись студентам.**

Если у нападающего холодное оружие рекомендуется:

1. **Оценить расстояние** от преступника до Вас и студентов, а также до выхода из помещения. Студенты, находящиеся ближе к выходу, могут рискнуть и выбежать.
2. **Держать нападающего в поле зрения.**
3. **В крайнем случае, попытаться отвлечь нападающего на себя и дать возможность спастись студентам.**

При действиях правоохранительных органов по нейтрализации преступников рекомендуется:

1. **Лежать на полу лицом вниз, голову закрыть руками и не двигаться.**
2. Ни в коем случае **не бежать навстречу сотрудникам спецслужб или от них**, так как они могут принять вас за преступника.
3. **Не брать в руки какие-либо предметы**, так как они могут быть восприняты как оружие.
4. Если есть возможность, **держаться подальше от проемов дверей и окон.**

При поджоге (возникновении пожара):

1. Выполнить мероприятия согласно инструкции по действиям при возникновении пожара.

При применении химических (отравляющих) и радиоактивных веществ:

1. **Организовать эвакуацию.** Оповестить посетителей, персонал, сообщить маршрут выхода в безопасное место.
2. **Организовать использование простейших средств индивидуальной защиты органов дыхания** (ватно-марлевые повязки, платки, шарфы, изделия из тканей, смоченные водой или содовым раствором).
3. **Организовать контроль за состоянием студентов и персонала.** При выявлении признаков поражения **передать пострадавших спасателям или медикам.**

При применении биологических веществ:

1. **Перекрыть все выходы из здания** (помещения), где совершено применение биологического вещества. Покидать здание кому-либо при применении биологических веществ строго запрещено, чтобы предотвратить распространение заражения.

2. **Установить на всех выходах посты охраны**, в т. ч. можно задействовать персонал университета.

3. **Прекратить доступ посетителей**, студентов и персонала в здание (помещение), где применено биологическое вещество, до прибытия специалистов служб.

4. **Отключить вентиляцию, кондиционеры, закрыть форточки, окна, двери.**

5. **Составить список лиц, находящихся в зоне поражения** (ФИО, домашние адреса, телефоны, места работы, должности). Передать списки сотрудникам служб, прибывшим для ликвидации последствий заражения.

6. **Выявить лиц, которые могли контактировать с опасным веществом**, и оказать им медицинскую помощь (при наличии антибиотиков).

Действия ректора, дежурного администратора, вахтера и меры безопасности при возникновении стрельбы

При возникновении стрельбы вблизи объекта (звуков выстрелов) или непосредственно на объекте необходимо немедленно дать сигнал тревоги посредством нажатия кнопки экстренного вызова полиции (КТС) (при наличии), затем сообщить в дежурную часть полиции по телефону.

Для соблюдения мер безопасности дать указание всему персоналу объекта и лицам, находящимся в это время на объекте, принять следующие меры предосторожности:

- не подходить и не стоять у окна, даже если оно закрыто занавеской;
- не подниматься выше уровня подоконника;
- не входить в помещения со стороны, которых слышны выстрелы;
- не пытаться задерживать незнакомых людей, т. к. они могут быть вооружены;
- оказать первую помощь пострадавшим, немедленно вызвать «скорую медицинскую помощь»;
- не открывать окна и двери, в случае если в них будут стучать;
- находясь в зоне стрельбы из огнестрельного оружия, лечь на землю и постараться отползти за укрытие (угол здания, клумба, бетонные плиты и ограждения, и т.п.), если такого поблизости нет, закрыть голову руками и лежать неподвижно;
- когда выстрелы прекратятся: подняться (с соблюдением мер предосторожности) и рассказать о том, что произошло прибывшим сотрудникам правоохранительных органов.

2 Действия при обнаружении взрывного устройства в почтовом отправлении

Основные признаки наличия в отправлении взрывной начинки: толщина письма от 3-х мм и выше, при этом в конверте (пакете, бандероли) есть отдельные утолщения; смещение центра тяжести письма к одной из его сторон; наличие в конверте перемещающихся предметов либо порошка; наличие во вложении металлических либо пластмассовых предметов; наличие на конверте масляных пятен, проколов, металлических кнопок; наличие необычного запаха (миндаля, жжёной пластмассы и др.); «тиканье» в бандеролях и посылках.

Вспомогательные признаки: тщательная заделка письма, бандероли, посылки, в том числе скотчем; подписи «лично в руки», «вскрыть только лично», «вручить лично» и т.п.; отсутствие обратного адреса, фамилии, неразборчивое их написание, вымышленный адрес;

4. нестандартная упаковка.

Порядок действий

1. При получении сообщения о заложенном взрывном устройстве, либо обнаружении предметов, вызывающих подозрение, немедленно поставьте в известность дежурных, дежурную часть ОВД. Сообщите адрес, телефон, фамилию, имя, отчество.

2. До прибытия оперативно-следственных органов, МЧС, пожарных принять меры к ограждению объекта на расстоянии, указанном в пункте 9.

3. По прибытии специалистов действовать в соответствии с их указаниями.

4. Не предпринимать действий, нарушающих состояние подозрительного предмета и других предметов, находящихся с ним в контакте.

5. Не допускать заливание водой, засыпку грунтом, покрытие плотными тканями.

6. Не пользоваться электро-, радиоаппаратурой, переговорными устройствами, рацией вблизи подозрительного предмета.

7. Не оказывать теплового, звукового, светового, механического воздействия на взрывоопасный предмет.

8. Не прикасаться к взрывоопасному предмету, находясь в одежде из синтетических волокон.

9. Рекомендуемые зоны эвакуации (и оцепления) при обнаружении взрывного устройства или предмета, подозрительного на взрывное устройство:

1 граната РГД-5 - 50 м,

2 граната Ф-1 - 200 м,

3 тротиловая шашка (200 г) - 45 м,

4 тротиловая шашка (400 г) - 55 м,

5 пивная банка (0,33 л) - 60 м,

6 мина (МОН-50) - 85 м,

7 чемодан (кейс) - 230 м,

8 дорожный чемодан - 250 м,

9 автомобиль «Жигули» - 460 м,

10 автомобиль «Волга» - 580 м,

11 микроавтобус - 920 м,

12 грузовик-фургон - 1240 м.

3 Действия при обнаружении подозрительных предметов, вещей

Минирование территории образовательного учреждения – наиболее вероятное проявление террористической деятельности.

Любое сообщение об обнаружении бесхозных вещей, подозрительных предметов или о минировании образовательного учреждения рассматривается как реальная угроза жизни людей, находящихся на предприятии.

Порядок действий при обнаружении подозрительных предметов:

- категорически запрещается трогать, вскрывать, передвигать или предпринимать какие-либо иные действия с обнаруженным предметом;
- не рекомендуется использовать мобильные телефоны и другие средства радиосвязи вблизи такого предмета;
- необходимо немедленно сообщить об обнаружении подозрительного предмета в полицию.

Если вы обнаружили неизвестный предмет:

1. Немедленно сообщите о находке администрации или охране;
2. Зафиксируйте время и место обнаружения;
3. Предпримите меры к тому, чтобы люди отошли как можно дальше от подозрительного предмета и опасной зоны;
4. Дождитесь прибытия представителей правоохранительных органов, укажите место расположения подозрительного предмета, время и обстоятельства его обнаружения;
5. Не паникуйте. О возможной угрозе взрыва сообщите только тем, кому необходимо знать о случившемся.

Необходимо помнить, что внешний вид предмета может скрывать его настоящее назначение. На наличие взрывного устройства, других опасных предметов могут указывать следующие признаки:

1. Присутствие проводов, небольших антенн, изолянты, шпагата, веревки, скотча в пакете, либо торчащие из пакета;
2. Шум из обнаруженных подозрительных предметов (пакетов, сумок и др.). Это может быть тиканье часов, щелчки и т.п.;
3. Наличие на найденном подозрительном предмете элементов питания (батареек);
4. Растяжки из проволоки, веревок, шпагата, лески;
5. Необычное размещение предмета;
6. Наличие предмета, несвойственного для данной местности;
7. Специфический запах, несвойственный данной местности.

В качестве камуфляжа для взрывных устройств используются обычные сумки, пакеты, свертки, коробки, игрушки и т.п.

Решение об эвакуации людей с территории объекта и ее степени принимается руководством территориальных органов УВД по результатам объективной оценки сведений об обнаруженных бесхозных вещах, подозрительных

предметах. О минировании образовательного учреждения сообщается через дежурную часть УВД в дежурную службу образовательного учреждения.

Дежурная часть УВД обязана передавать полную информацию о минировании образовательного учреждения, поступившую из централизованных источников и др., а также о принимаемых по этим фактам мерах (вызов кинолога, саперов и т.д.), по фактам обнаружения бесхозных вещей или подозрительных предметов и об окончании выполнения этих мероприятий.

Выполнение мероприятий по эвакуации обеспечивается совместными действиями сотрудников территориальных органов УВД, охраны, должностных лиц и работников образовательного учреждения.

Руководитель образовательного учреждения и дежурная служба перемещаются в район сбора эвакуируемых, оповещают об этом дежурную часть УВД, должностных лиц образовательного учреждения и продолжают выполнять свои функциональные обязанности, используя мобильную связь, рации или посыльных из числа эвакуированных работников образовательного учреждения.

Степени эвакуации в зависимости от нарастания обстановки могут вводиться последовательно или независимо.

4 Алгоритм действия работников при получении подозрительных почтовых отправлений

Основными характерными признаками "подозрительных" писем (бандеролей) указывающих на угрозу (предпосылки) возникновения террористического акта биологического, радиационного и химического происхождения, являются:

- неожиданный для учреждения адресат;
- оформление детским почерком почтового отправления с адресатом в государственный орган исполнительной власти;
- письмо (бандероль) адресовано сотруднику, уже не работающему в данном учреждении, или имеются еще какие-либо неточности в адресе;
- письмо (бандероль) не имеет обратного адреса или имеет неправильный обратный адрес;
- почтовая марка на конверте не соответствует городу (государству) в обратном адресе;
- письмо (бандероль) помечено ограничениями типа "Лично" и "Конфиденциально";
- конверт (упаковка бандероли) необычен по форме, весу, размеру, неровен по бокам и т.д.;
- конверты (упаковка бандероли) имеют странный запах или цвет, в них прощупываются посторонние вложения;
- визуальное (при «просвете» письма с использованием яркого источника света: солнечный свет, лампа, пр.) или тактильное (на ощупь без вскрытия конверта) определение наличия в «подозрительном» письме, порошкообразного вещества.

Действия работника, осуществляющего работу с почтовыми отправлениями, при получении письма (бандероли) с подозрительными признаками:

- не вскрывать конверт (бандероль);
- положить его в пластиковый пакет, а в другой пластиковый пакет – лежащие в непосредственной близости с письмом (бандеролью) предметы;
- при повреждении конверта или вскрытии его и просыпании на стол (пол) находящегося в нем порошкообразного вещества, положить конверт на просыпанное вещество и накрыть его пластиковым пакетом;
- убедиться, что "подозрительная" или поврежденная почта отделена от других писем и бандеролей и ближайшая к ней поверхность ограничена;
- вымыть руки водой с мылом и убедиться, что все, кто трогал "подозрительное" письмо (бандероль), также вымыли руки водой с мылом;
- незамедлительно доложить о факте получения "подозрительного" письма (бандероли) руководителю учреждения (организации) и в дальнейшем действовать по его указанию.

Действия руководителя при получении информации о поступлении почтовой корреспонденции (писем, бандеролей, посылок) с подозрительной субстанцией, а также информации об обнаружении подозрительных жидкостей, россыпей порошкообразных веществ в подъездах, вестибюле, лифтах, кабинетах, помещениях, во внутреннем дворе и по наружному периметру территории:

- немедленно информирует дежурную часть территориального подразделения МВД РФ и территориальное подразделение Управления Роспотребнадзора

ра о месте и характеристике обнаружения признаков террористической угрозы радиационного, химического или биологического происхождения (контактные телефоны заранее согласовываются и вносятся в схему оповещения при возникновении (угрозе возникновения) теракта РХБ происхождения);

- до прибытия представителей МВД организует оцепление места обнаружения подозрительного предмета;

- исключает допуск в очаг потенциального заражения (загрязнения) посторонних лиц;

- ограничивает передвижение сотрудников учреждения (организации) внутри объекта;

- дает распоряжения о составлении списка лиц, контактировавших с неизвестной субстанцией (веществом);

- запрещает выход сотрудников и посетителей, контактировавших с неизвестной субстанцией (веществом) за пределы учреждения (организации);

- обеспечивает допуск прибывших формирований МВД, МЧС, др. уполномоченных организаций для выполнения задач по предназначению, а также учреждений Роспотребнадзора для отбора подозрительного материала на исследование и выполнения других противоэпидемиологических мероприятий;

- выполняет и организует выполнение дальнейших распоряжений и указаний, только после их согласования с прибывшими сотрудниками Управления Роспотребнадзора или его структурных подразделений, уполномоченных на решение задач направленных на минимизацию последствий возникновения (угрозы возникновения) террористического акта радиационного, химического и биологического происхождения;

- поддерживает постоянную связь с Управлением Роспотребнадзора или его территориальными подразделениями и с дежурной частью территориального подразделения МВД РФ по автономному округу;

- осуществляет постоянное наблюдение за развитием ЧС, ходом выполнения работ по ликвидации медико-санитарных последствий, включая проведения дезинфекционных мероприятий (первичная, повторная, заключительная дезобработка), до их полного завершения.

Рекомендации сотрудникам по профилактике заражения биологической субстанцией в результате предполагаемого биологического террористического акта:

1. Не принимать за пределами или в помещениях здания писем, пакетов, бандеролей, посылок и т.п. для передачи руководству или другим сотрудникам от незнакомых Вам людей (посетителей учреждения).

2. При обнаружении в подъездах, вестибюле, лифтах, кабинетах и других помещениях, а также во внутреннем дворе и по наружному периметру территории подозрительных жидкостей, россыпей порошкообразных веществ, проинформировать об этом дежурного, а при его отсутствии руководителя.

3. Избегать самому и другим работникам контакта с подозрительными субстанциями.

4. Беспрекословно выполнять распоряжения руководства учреждения и прибывших специалистов Управления Роспотребнадзора по автономному округу или его территориальных подразделений, относящихся к профилактике биологического заражения и ликвидации медико-санитарных последствий возможного биологического террористического акта на территории учреждения.

5 Порядок действий при получении сообщений, содержащих угрозы террористического характера

После сообщения по телефону об угрозе взрыва, о наличии взрывного устройства не впадать в панику. Быть выдержанными и вежливыми, не прерывать говорящего. При наличии магнитофона надо поднести его к телефону, записать разговор. Постараться сразу дать знать об этой угрозе своему коллеге, по возможности одновременно с разговором он должен по другому аппарату сообщить оперативному дежурному милиции и дежурному по отделу ФСБ о поступившей угрозе и номер телефона, по которому позвонил предполагаемый террорист.

Предупредительные меры при поступлении угрозы террористического акта по телефону:

1. Инструктировать дежурный персонал о порядке приема телефонных сообщений с угрозами террористического акта;
2. После сообщения по телефону об угрозе взрыва, о наличии взрывного устройства не впадать в панику;
3. Не распространять о факте разговора и его содержании;
4. Максимально ограничить число людей, владеющих полученной информацией.

Действия при получении телефонного сообщения об угрозе террористического акта:

1. Реагировать на каждый поступивший телефонный звонок;
2. Постараться дать знать об этой угрозе своему коллеге, по возможности одновременно с разговором он должен по другому аппарату сообщить оперативному дежурному милиции по телефону 02 о поступившей угрозе, а также ректору университета;
3. При необходимости эвакуировать людей в соответствии с планом эвакуации;
4. Обеспечить беспрепятственную работу оперативно-следственной группы.

В любом случае постарайтесь в ходе разговора получить ответы на следующие вопросы:

- куда, кому, по какому телефону звонит этот человек?
- какие конкретные требования он (она) выдвигает?
- выдвигает требования он (она) лично, выступает в роли посредника или представляет какую-либо группу лиц?
- на каких условиях он (она) или они согласны отказаться от задуманного?
- как и когда с ним (с ней) можно связаться?
- кому вы можете или должны сообщить об этом звонке?

Постарайтесь добиться от звонящего максимально возможного промежутка времени для принятия вами и вашим руководством решений или совершения каких-либо действий.

Действия при принятии телефонного сообщения об угрозе взрыва.

Будьте спокойны, вежливы, не прерывайте говорящего. Сошлитесь на некачественную работу аппарата, чтобы записать разговор. Не вешайте телефонную трубку по окончании разговора.

1. Постарайтесь дословно запомнить разговор и зафиксировать его на бумаге.

2. По ходу разговора отметьте пол, возраст звонившего и особенности его (ее) речи:

- голос: громкий, тихий, низкий, высокий;

- темп речи: быстрая, медленная;

- произношение: отчетливое, искаженное, с заиканием, с заиканием шепелявое, с акцентом или диалектом;

- манера речи: развязная, с издевкой, с нецензурными выражениями.

3. Отметьте звуковой фон (шум автомашин или железнодорожного транспорта, звуки теле- или радиоаппаратуры, голоса, другое).

4. Отметьте характер звонка (городской или междугородный).

5. Зафиксируйте точное время начала разговора и его продолжительность.

6. Постарайтесь добиться от звонящего максимально возможного промежутка времени для принятия Вами и Вашим руководством решений или совершения каких-либо действий;

8. При наличии автоматического определителя номера запишите определившийся номер телефона;

9. При использовании звукозаписывающей аппаратуры сразу же извлеките кассету (минидиск) с записью разговора и примите меры к ее сохранности;

10. Не задавайте провоцирующие вопросы (об имени звонящего, местонахождении и т.д.), т.к. они могут заставить звонящего прекратить разговор;

11. Постарайтесь в ходе разговора получить ответы на следующие вопросы:

1. Когда может быть проведен взрыв?

2. Где заложено взрывное устройство?

3. Что оно из себя представляет?

4. Как оно выглядит внешне?

5. Есть ли еще где-нибудь взрывное устройство?

6. Для чего заложено взрывное устройство?

7. Каковы ваши требования?

8. Вы один или с вами есть еще кто-либо?

6 Порядок действий персонала и обучающихся по действиям при захвате заложников

Любой человек по стечению обстоятельств может оказаться заложником у преступников, и он должен точно представлять, как он будет себя вести и каковы его возможные действия, быть психологически устойчив. При этом преступники могут добиваться достижения политических целей, получения выкупа и т.п.

Во всех случаях ваша жизнь становится предметом торга для террористов.

Действия персонала и обучающихся при сообщении о захвате заложников:

1. При захвате заложников необходимо незамедлительно сообщить в правоохранительные органы о сложившейся в школе ситуации.

2. В ситуации, когда проявились признаки угрозы захвата в заложники вас, постарайтесь избежать попадания в их число. С этой целью немедленно покиньте опасную зону или спрячьтесь.

3. Спрятавшись, дождитесь ухода террористов и при первой возможности покиньте убежище. Исключением являются ситуации, когда вы оказались в поле зрения террористов или когда высока вероятность встречи с ними.

4. Не вступайте в переговоры с террористами по собственной инициативе.

5. Примите меры к беспрепятственному проходу (проезду) на объект сотрудников правоохранительных органов, МЧС, автомашин скорой медицинской помощи.

6. По прибытии сотрудников спецподразделений ФСБ и МВД окажите помощь в получении интересующей их информации.

Будьте внимательны, постарайтесь запомнить приметы преступников, отличительные черты их лиц, одежду, имена, клички, возможные шрамы и татуировки, особенности речи и манеры поведения, тематику разговоров и т.п.

Если Вас захватили в качестве заложника, помните, что Ваше собственное поведение может повлиять на обращение с Вами:

1. При необходимости выполнять требования преступников, если это не связано с причинением ущерба жизни и здоровью людей, не спорьте с террористами.

2. Не допускать действий, которые могут спровоцировать нападающих к применению оружия и привести к человеческим жертвам.

3. Перенося лишения, оскорбления и унижения, не смотрите в глаза преступникам, не ведите себя вызывающе.

4. При необходимости совершить то или иное действие (сесть, встать, попить, сходить в туалет), спрашивайте разрешение.

5. Если вы ранены, то постарайтесь не двигаться. Этим вы сократите потерю крови.

6. Помните: ваша цель — остаться в живых.

7. Будьте внимательны, постарайтесь запомнить приметы преступников, отличительные черты их лиц, одежду, имена, клички, возможные шрамы и татуировки, особенности речи и манеры поведения, тематику разговоров и т.д.

8. Помните, что, получив сообщение о вашем захвате, спецслужбы уже начали действовать и предпримут все необходимое для вашего освобождения.

9. Будьте готовы к применению террористами повязок на глаза, кляпов, наручников или веревок.

10. Не пытайтесь оказывать сопротивление, не проявляйте ненужного героизма, пытайтесь разоружить бандита или прорваться к выходу или окну.

11. Если вас заставляют выйти из помещения, говоря, что вы взяты в заложники, не сопротивляйтесь.

12. Если с вами находятся дети, найдите для них безопасное место, постарайтесь закрыть их от случайных пуль, по возможности находите рядом с ними.

13. В случае когда необходима медицинская помощь, говорите спокойно и кратко, не нервирова бандитов, ничего не предпринимайте, пока не получите разрешения.

14. Будьте настороже. Сосредоточьте Ваше внимание на звуках, движениях и т.п.

15. Займитесь умственными упражнениями. Не давайте ослабнуть своему сознанию. Насколько позволяют силы и пространство помещения занимайтесь физическими упражнениями.

16. Будьте готовы к "спартанским" условиям жизни: неадекватной пище и условиям проживания; неадекватным туалетным удобствам.

17. Если есть возможность, обязательно соблюдайте правила личной гигиены.

18. При наличии проблем со здоровьем, убедитесь, что Вы взяли с собой необходимые лекарства, сообщите охранникам о проблемах со здоровьем, при необходимости просите об оказании медицинской помощи или предоставлении лекарств.

19. Будьте готовы объяснить наличие у Вас каких-либо документов, номеров телефонов и т.п.

20. Если Вам дали возможность поговорить с родственниками по телефону, держите себя в руках, не плачьте, не кричите, говорите коротко и по существу. Попробуйте установить контакт с охранниками. Объясните им, что Вы тоже человек. Покажите им фотографии членов Вашей семьи. Не старайтесь обмануть их.

21. Если охранники на контакт не идут, разговаривайте как бы сами с собой, читайте вполголоса стихи или пойте.

22. Обязательно ведите счет времени, отмечая с помощью спичек, камешков или черточек на стене прошедшие дни.

23. Если вы оказались запертыми в каком-либо помещении, то постарайтесь привлечь чье-либо внимание. Для этого разбейте оконное стекло и позовите на помощь, при наличии спичек подожгите бумагу и поднесите ближе к пожарному датчику и т.п.

24. Никогда не теряйте надежду на благополучный исход. Помните, чем больше времени пройдет, тем больше у Вас шансов на спасение.

25. Во время проведения спецслужбами операции по вашему освобождению неукоснительно соблюдайте следующие требования:

- лежите на полу лицом вниз, голову закройте руками и не двигайтесь;
- ни в коем случае не бегите навстречу сотрудникам спецслужб или от них, так как они могут принять вас за преступника;
- если есть возможность, держитесь подальше от проемов дверей и окон.

7 Правила обращения с анонимными материалами, содержащими угрозы террористического характера

При получении анонимного материала, содержащего угрозы террористического характера, обращайтесь с ним максимально осторожно, уберите его в чистый плотно закрываемый полиэтиленовый пакет и поместите в отдельную жесткую папку.

Постарайтесь не оставлять на нем отпечатков своих пальцев.

Сохраняйте все: сам документ с текстом, любые вложения, конверт и упаковку ничего не выбрасывайте.

Не расширяйте круг лиц, знакомившихся с содержанием документа.

Анонимные материалы направьте в правоохранительные органы с сопроводительным письмом, в котором должны быть указаны конкретные признаки анонимных материалов (вид, количество, каким способом и на чем исполнены, с каких слов начинается и какими заканчивается текст, наличие подписи и т. п.), а также обстоятельства, связанные с их распространением, обнаружением или получением.

Анонимные материалы не должны сшиваться, склеиваться, на них не разрешается делать подписи, подчеркивать или обводить отдельные места в тексте, писать резолюции и указания, также запрещается их мять и сгибать.

При исполнении резолюции и других надписей на сопроводительных документах не должно оставаться давленных следов на анонимных материалах.

Регистрационный штамп проставляется только на сопроводительных письмах организации и заявлениях граждан, передавших анонимные материалы в инстанции.

8 Памятка по действиям сотрудников ФГБОУ ВО Брянский ГАУ при поступлении угроз террористического характера посредством электронных почтовых сервисов международной информационно-коммуникационной сети Интернет

Общие сведения Памятка по действиям сотрудников при поступлении угроз террористического характера посредством электронных почтовых сервисов международной информационно-коммуникационной сети Интернет (далее - Памятка) была разработана в связи с участвовавшими случаями рассылки по организациям писем с угрозами о совершении преступлений террористического характера. В настоящей Памятке содержатся рекомендации по действиям сотрудников при получении по электронной почте различных интернетресурсов, предоставляющих услуги электронной почты, 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, сотрудникам необходимо обеспечить условия, способствующие сохранению полученной информации с последующим обязательным информированием правоохранительных органов о получении указанных сообщений.

ПАМЯТКА

**ПО ДЕЙСТВИЯМ СОТРУДНИКОВ ФГБОУ ВО БРЯНСКИЙ ГАУ
ПРИ ПОСТУПЛЕНИ УГРОЗ ТЕРРОРЕСТИЧЕСКОГО ХАРАКТЕРА
ПОСРЕДСТВОМ ЭЛЕКТРОННЫХ ПОЧТОВЫХ СЕРВИРОВ
МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННО-КОММУНИКАЦИОННОЙ
СЕТИ ИНТЕРНЕТ**

Общие сведения

Памятка по действиям сотрудников при поступлении угроз террористического характера посредством электронных почтовых сервисов международной информационно-коммуникационной сети Интернет (далее - Памятка) была разработана в связи с участвовавшими случаями рассылки по организациям писем с угрозами о совершении преступлений террористического характера.

В настоящей Памятке содержатся рекомендации по действиям сотрудников при получении по электронной почте различных интернетресурсов, предоставляющих услуги электронной почты, 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, сотрудникам 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

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

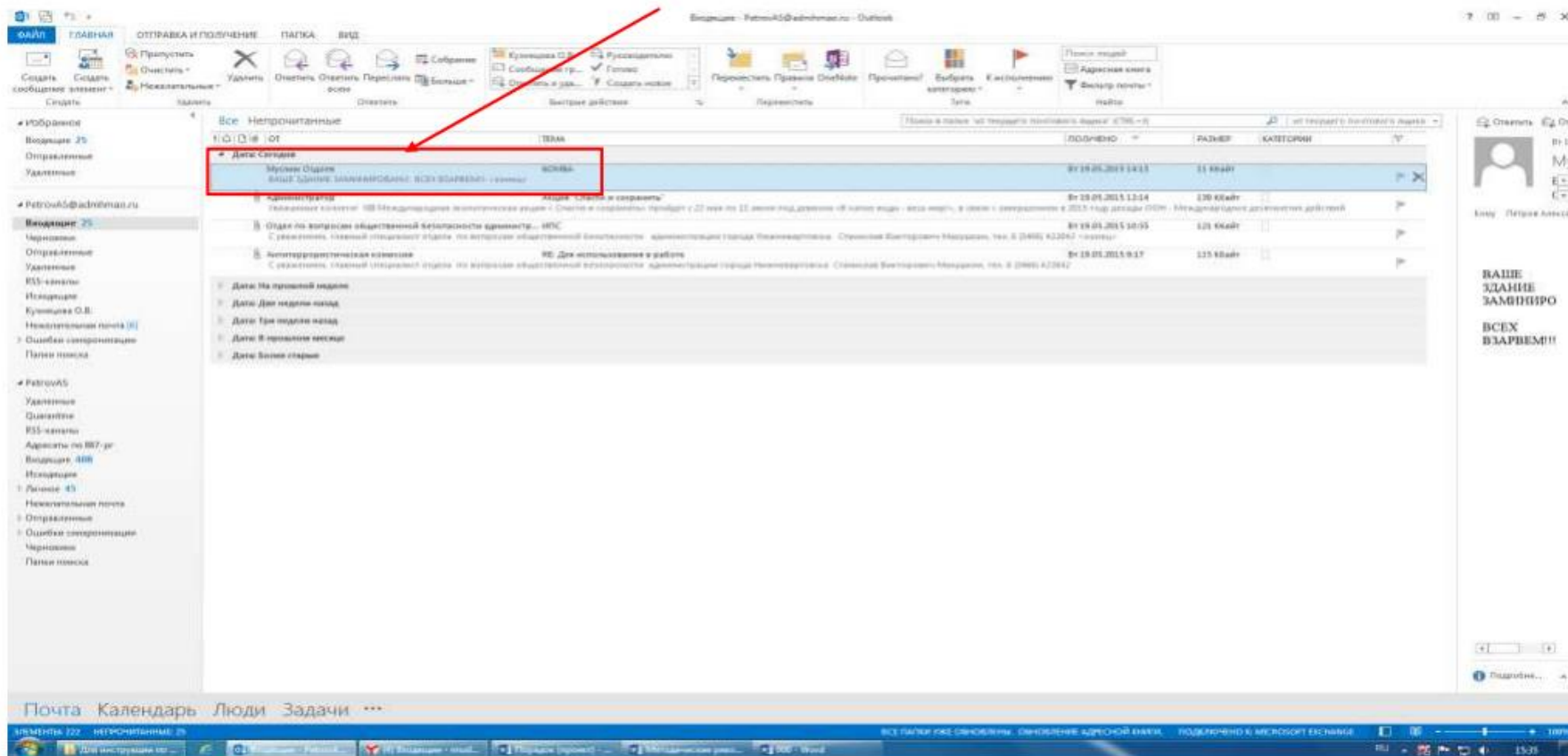


Рис. 1. – Вид сообщения

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).

20

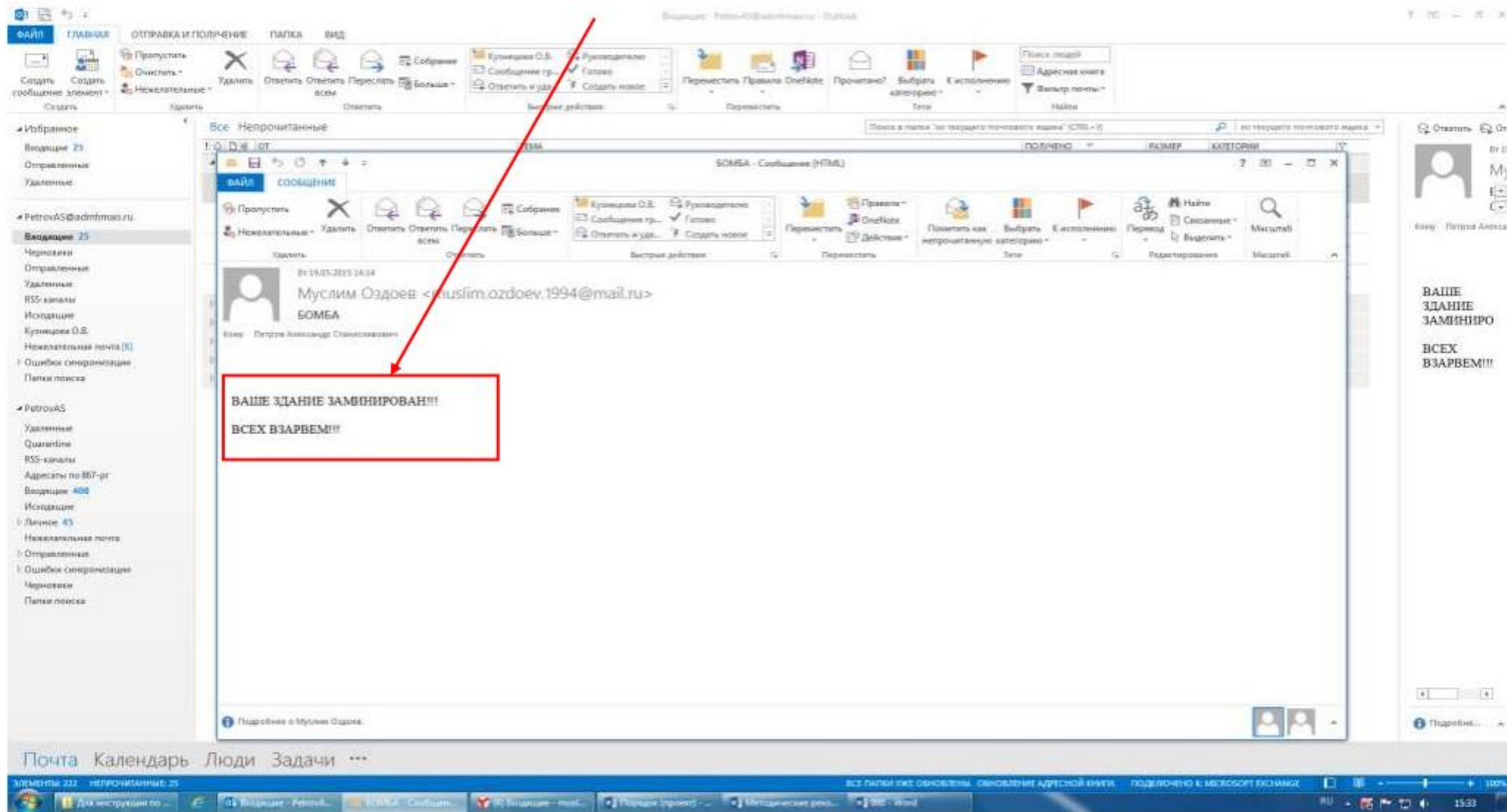


Рис. 2. – Сообщение в открытом окне

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).

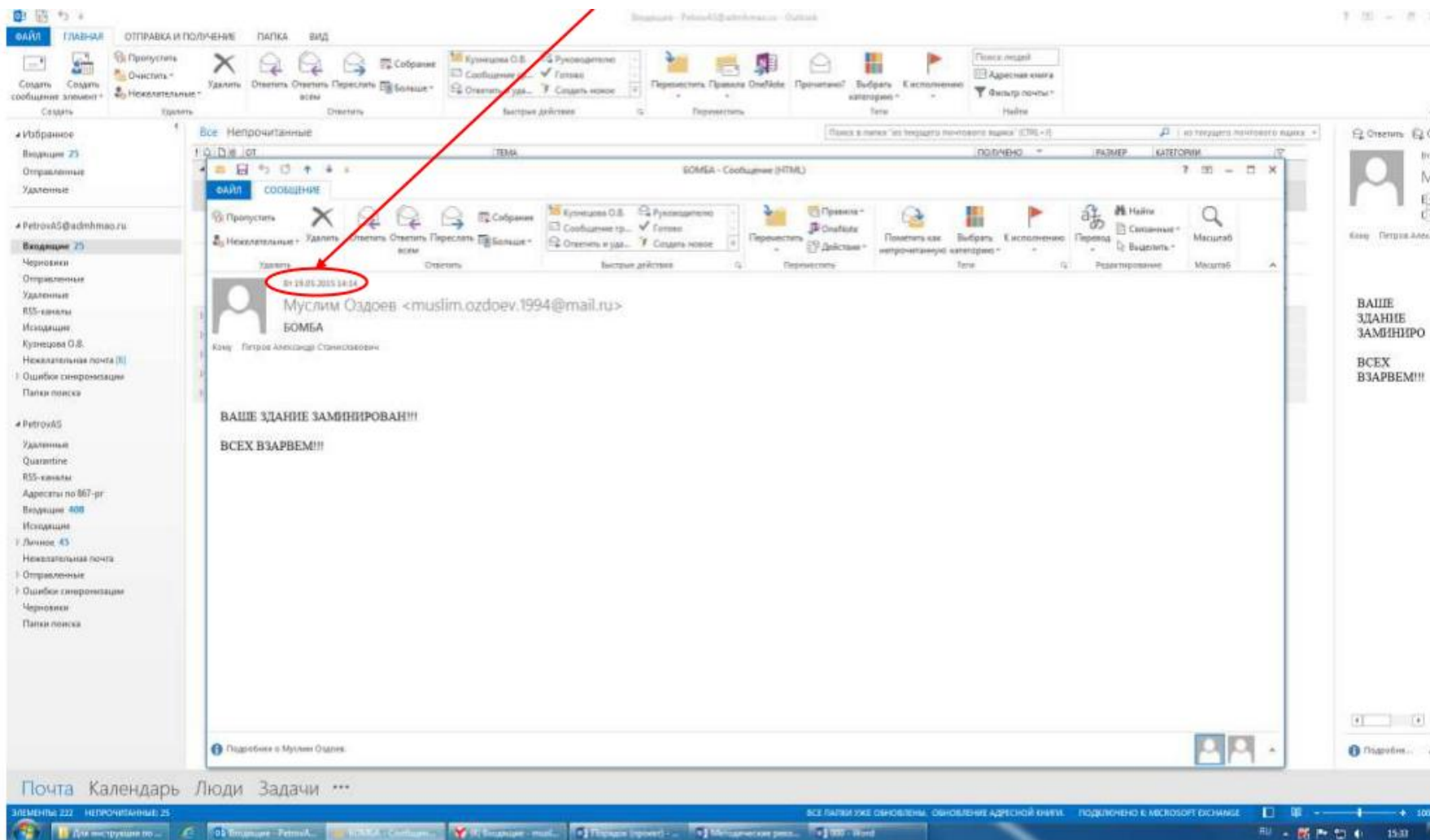


Рис. 3. – Дата полученного сообщения

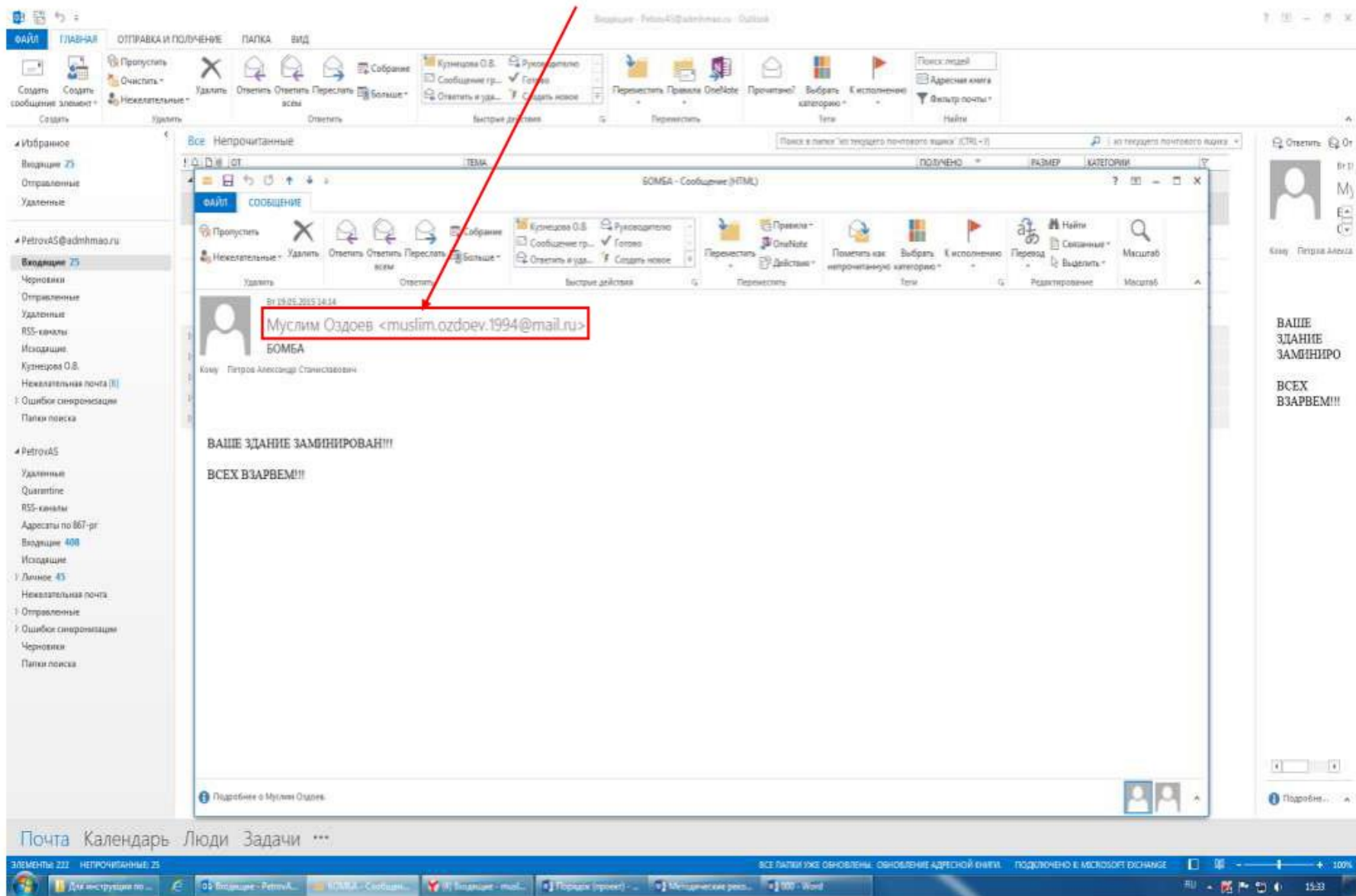


Рис. 4. – Имя и электронный адрес отправителя сообщения

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).

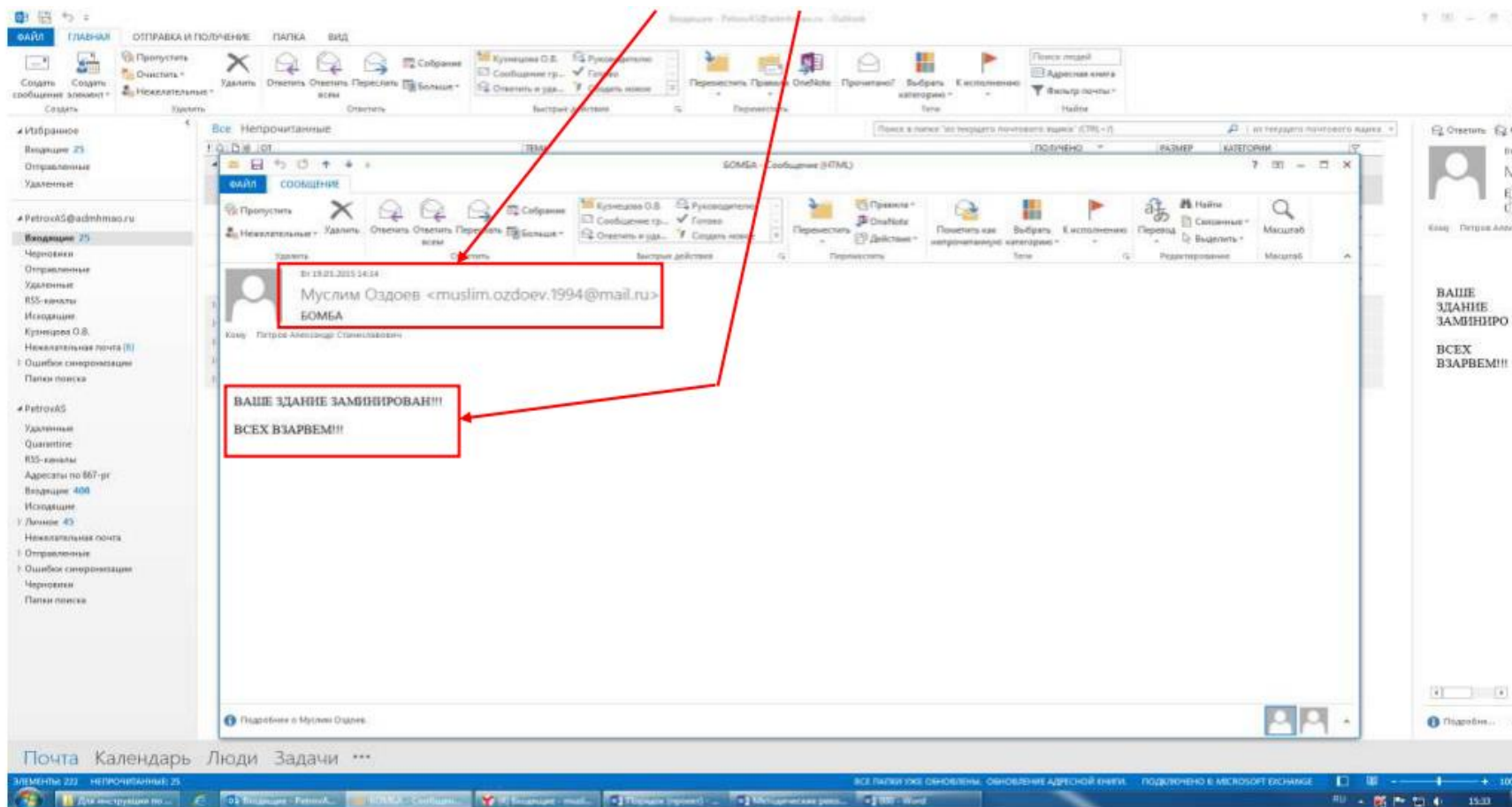


Рис. 5 – Информация в открытом окне полученного сообщения

Для копирования полученной информации необходимо сделать скриншот (снимок экрана). На клавиатуре для этих целей предусмотрена специальная клавиша «PrintScreen» («печать экрана»), которая, как правило, находится в верхнем ряду вместе с клавишами «ScrollLock» («изначальная функция») и «Pause/ Break» («приостанавливать/прерывать»), справа от клавиши «F12» (рис. 6).

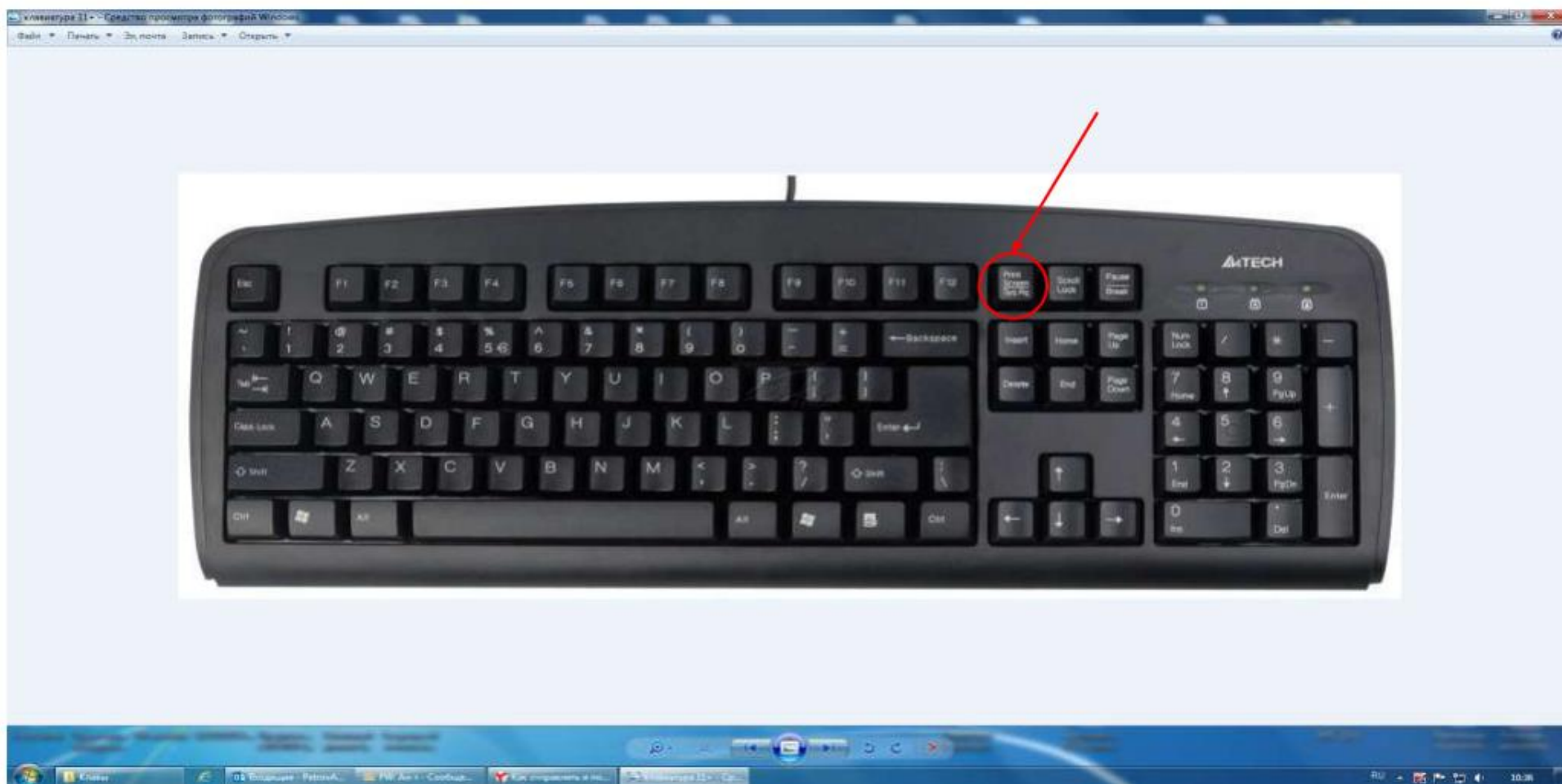


Рис. 6 – Расположение клавиши «PrintScreen» на клавиатуре компьютера

В зависимости от версии дизайнеров клавиатур кнопка с таким названием может быть следующих видов:



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».

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

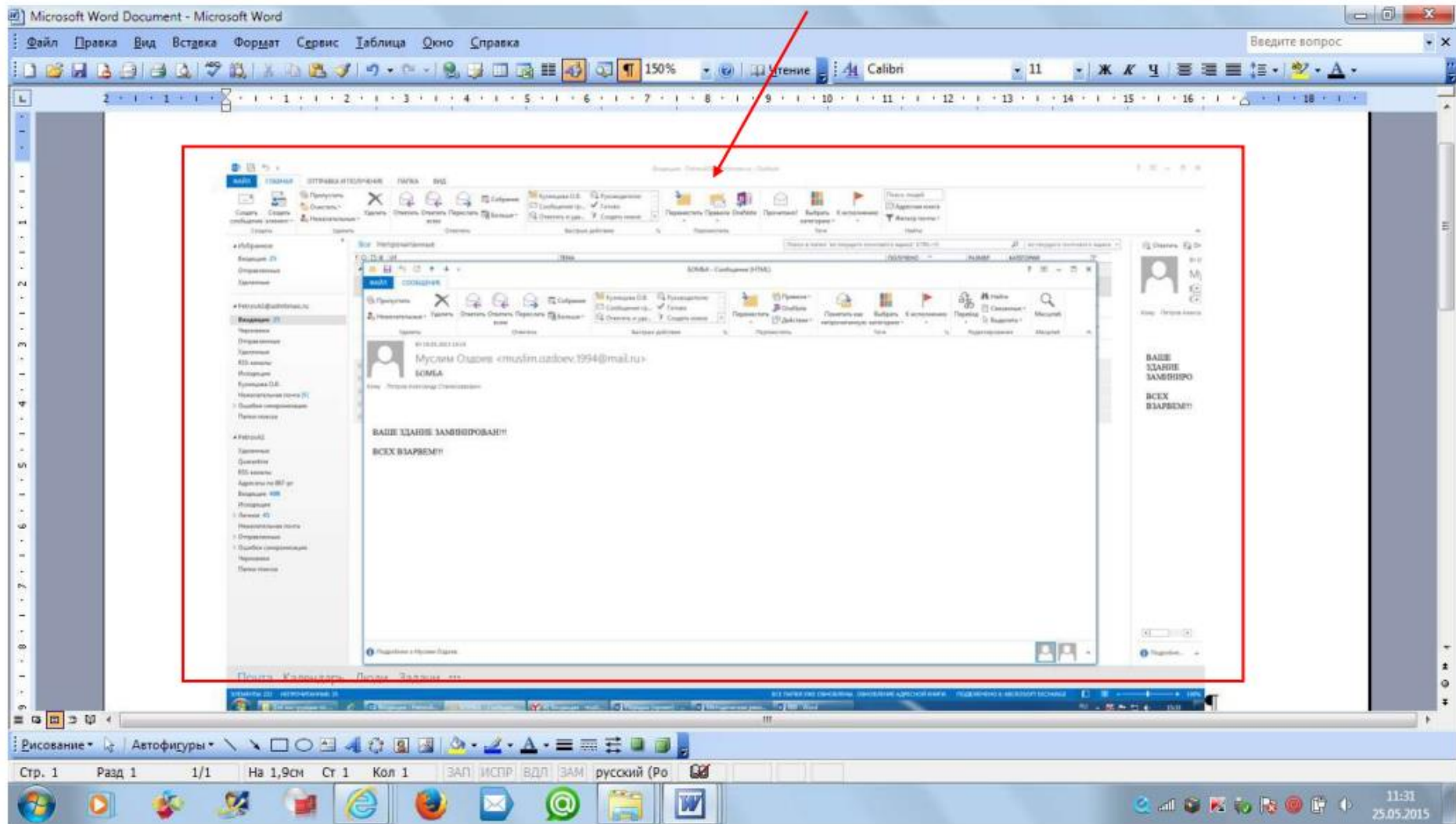


Рис. 8 – Размещение скриншота в созданном документе «MicrosoftWordDocument»

По завершению вышеуказанных действий сохраняем размещённый скриншот снимка экрана в созданном документе «Microsoft Word Document». Для этого необходимо нажать знак «Сохранить» на верхней панели документа «MicrosoftWordDocument» (рис. 9) или закрыть документ с подтверждением сохранения при открытии активного диалогового окна (рис. 10).

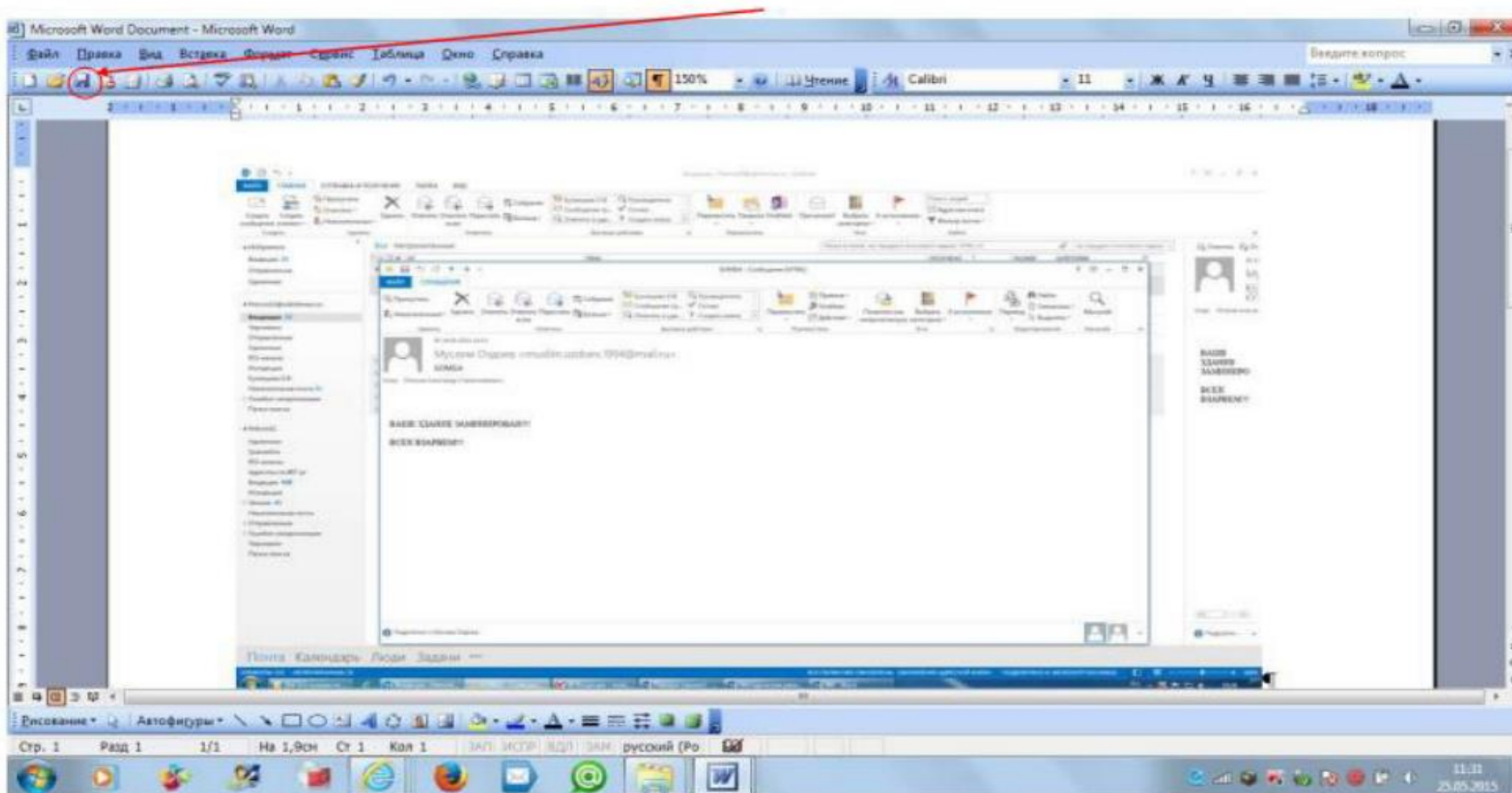


Рис. 9 – Сохранение скриншота в созданном документе «MicrosoftWordDocument».

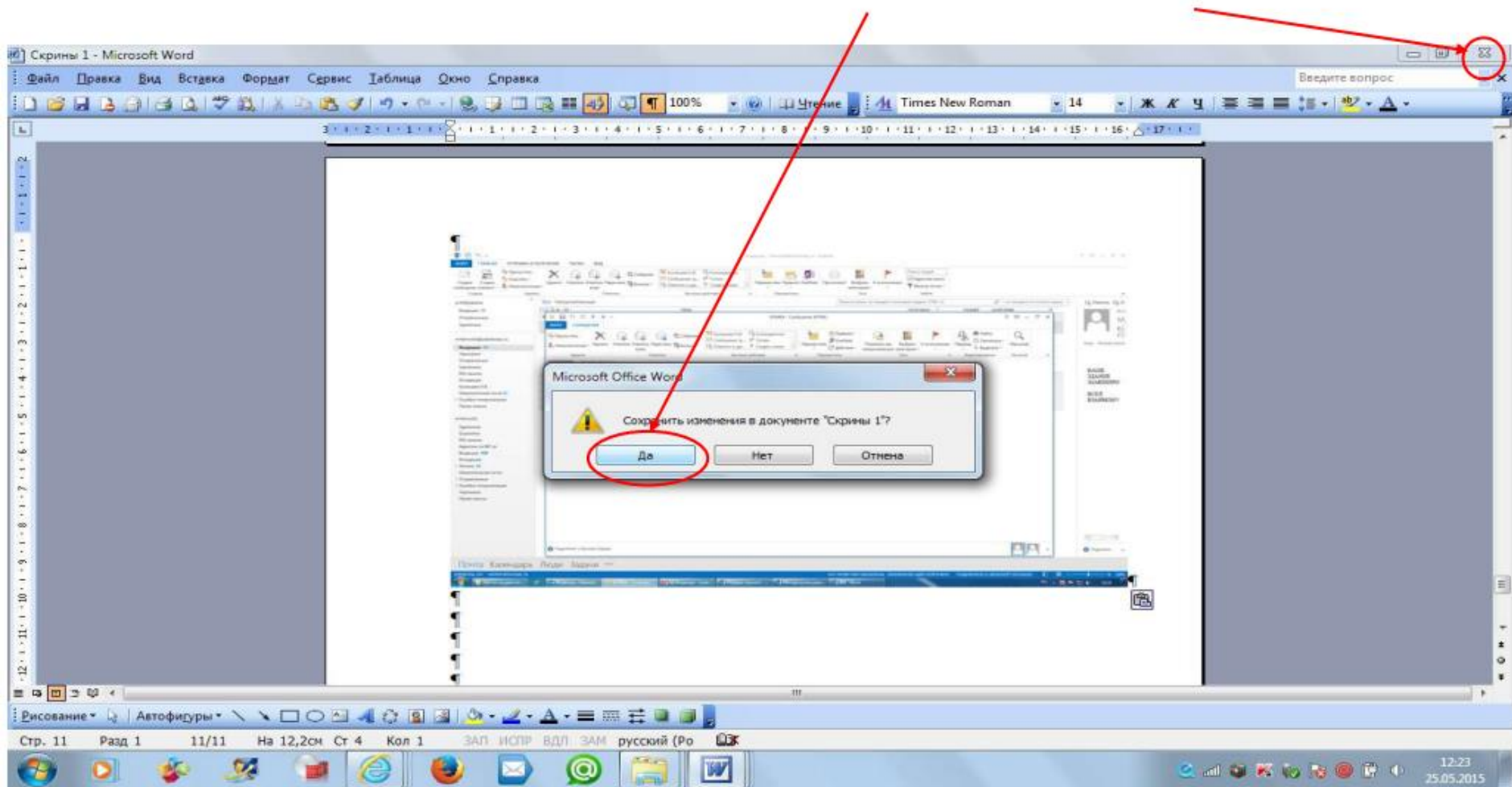


Рис. 10 – Сохранение скриншота в созданном документе «MicrosoftWordDocument».

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» (рис. 11а, 11б) или в пространстве нижней части окна сообщения (рис. 12).

30

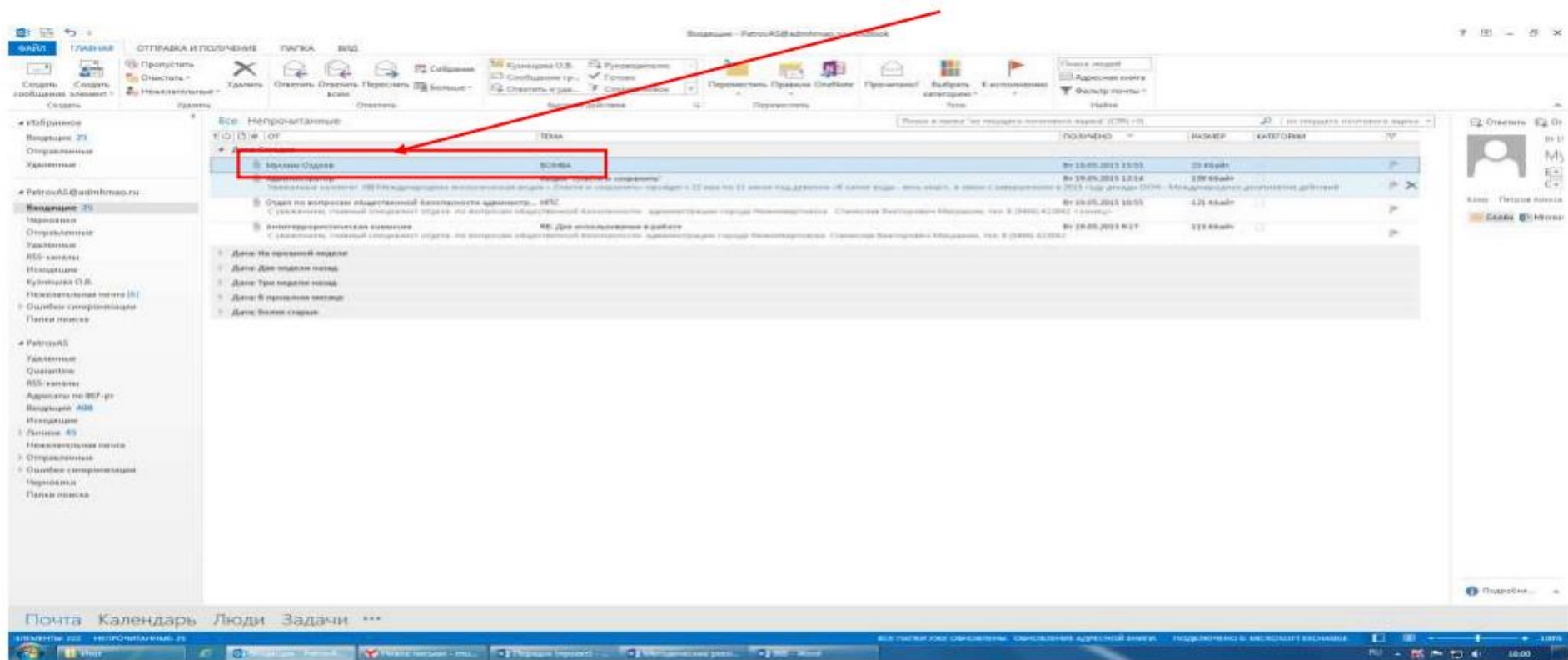


Рис. 11а – Письмо, содержащее вложение, содержит в поле «Тема» явные признаки угрозы террористического характера

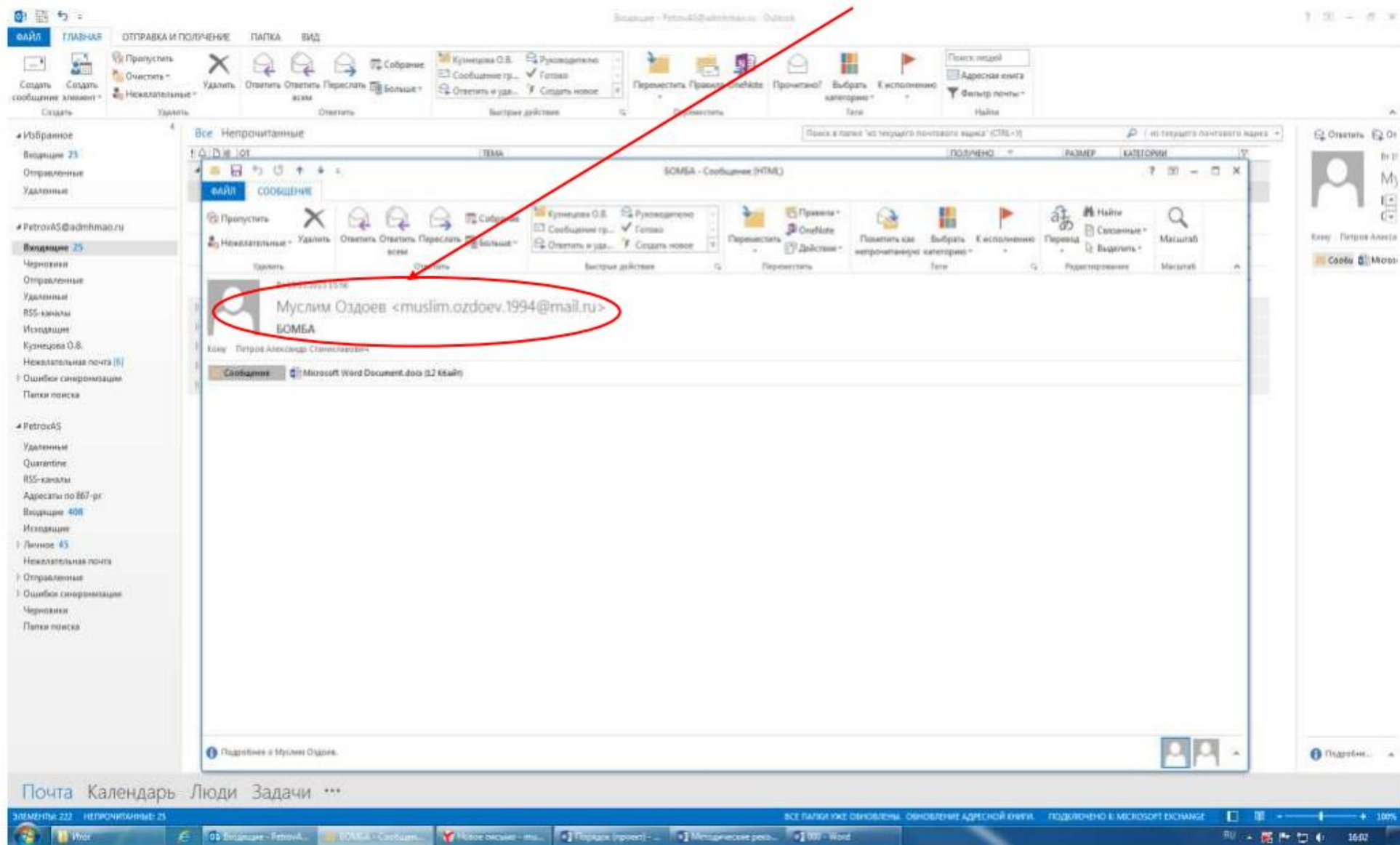


Рис. 11б – Письмо, содержащее вложение, содержит в поле «Тема» явные признаки угрозы террористического характера

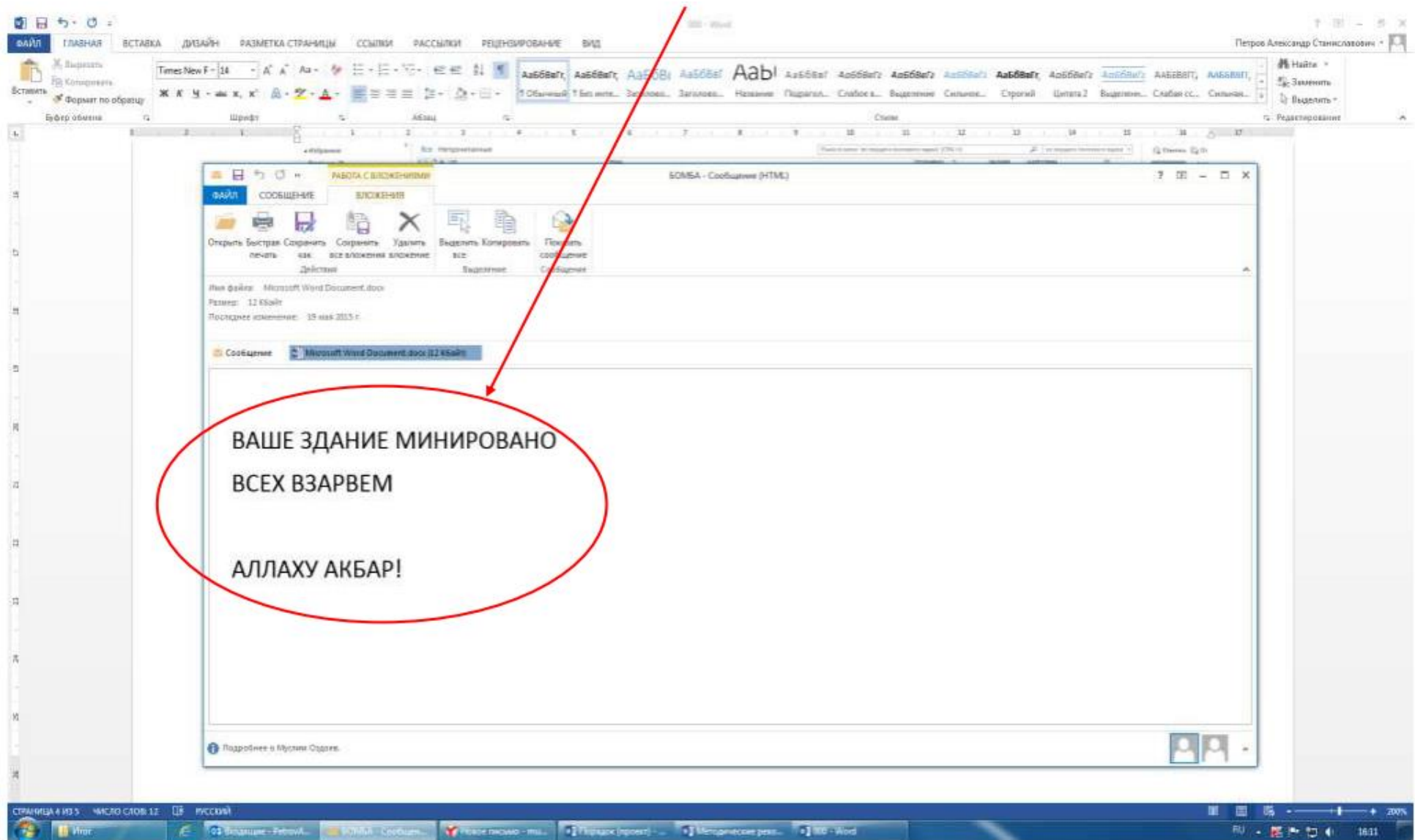


Рис. 12 – Письмо, содержащее вложение, содержит в пространстве нижней части окна сообщения явные признаки угрозы террористического характера

2.2. В письме, содержащем вложение, могут отсутствовать в поле «Тема» или в пространстве нижней части окна сообщения явные признаки угрозы совершения террористического акта (рис. 13а, 13б).

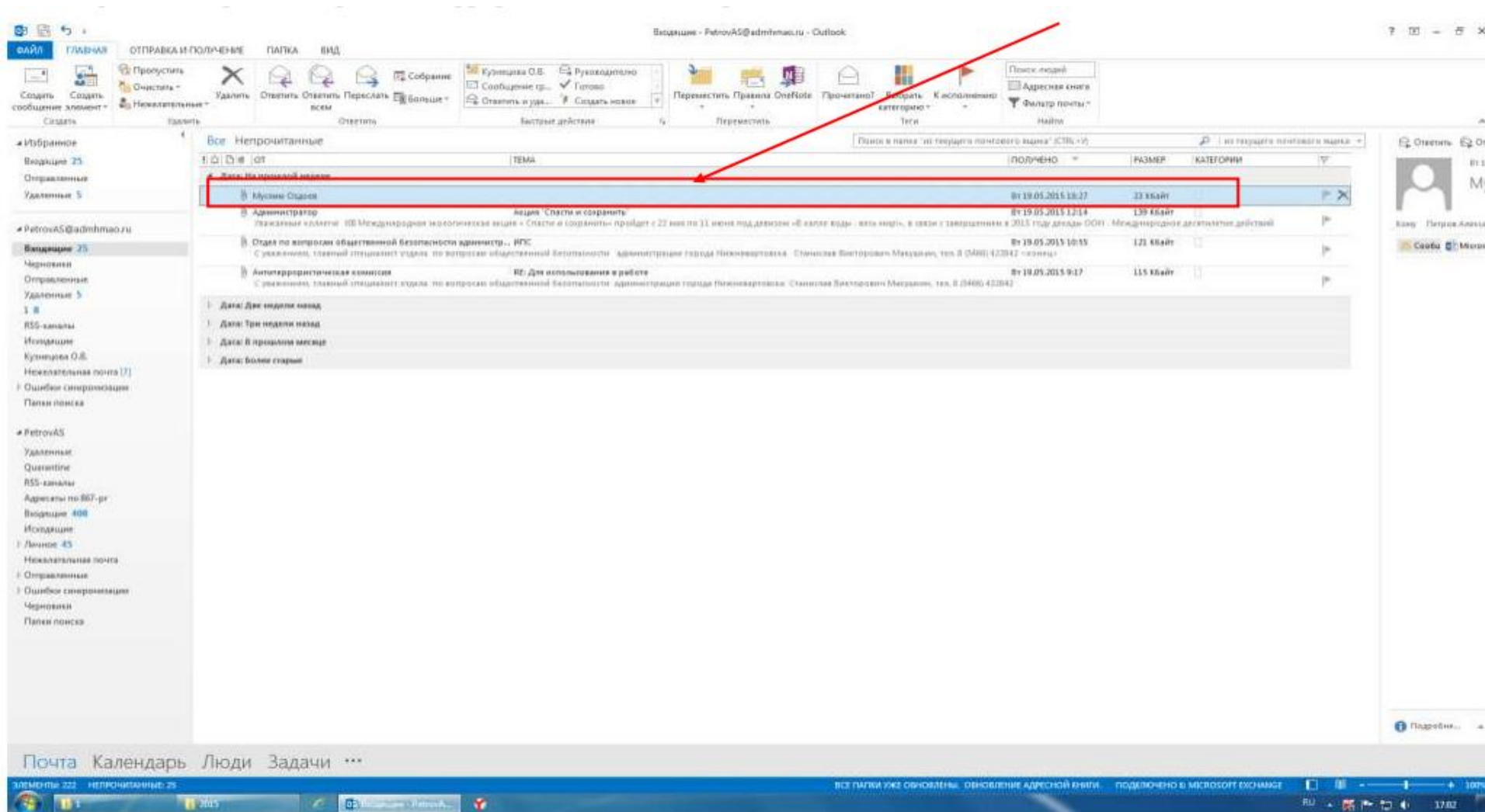


Рис. 13а – В письме, содержащем вложение, в поле «Тема» явные признаки угрозы террористического характера отсутствуют

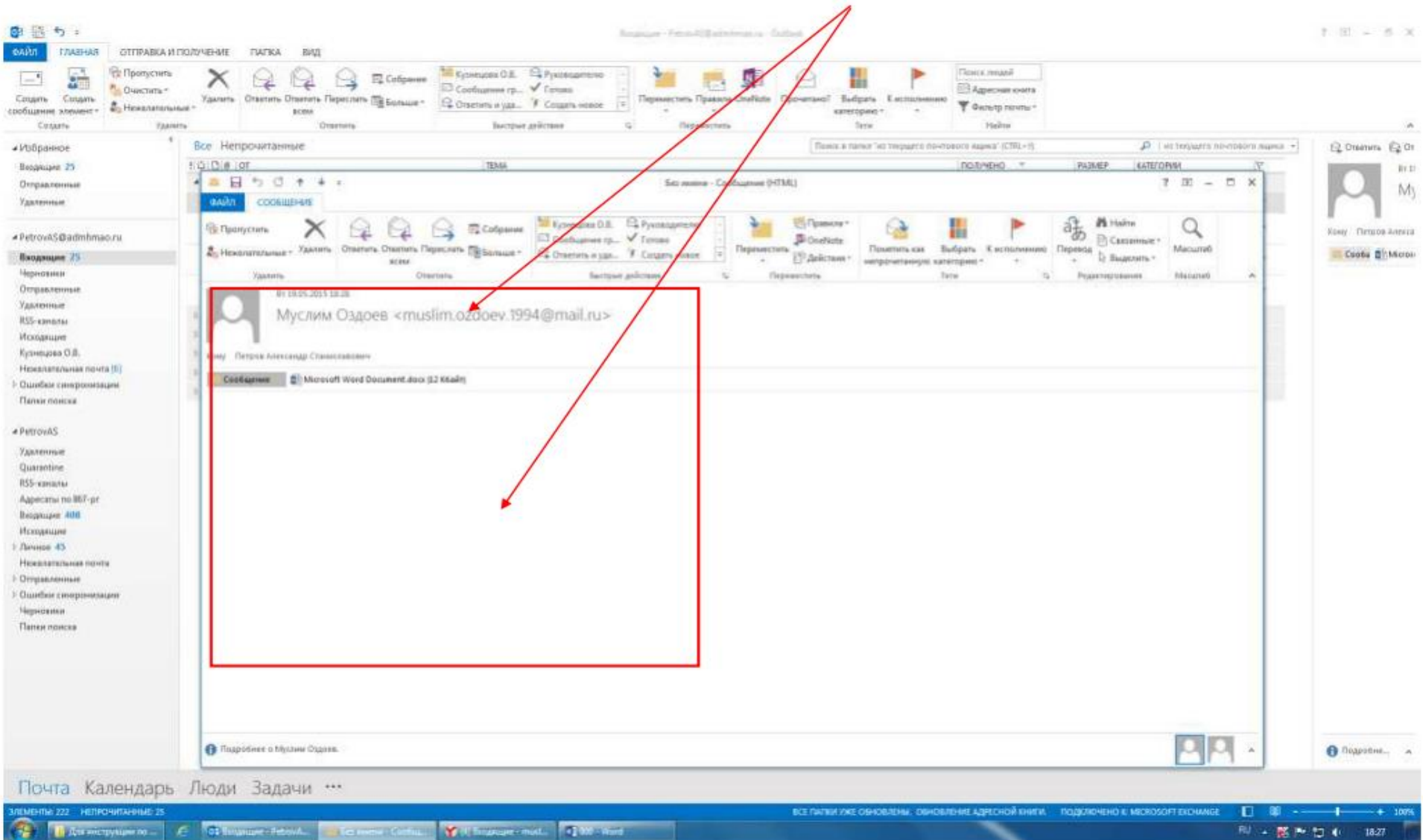


Рис. 136 – В письме, содержащем вложение, в пространстве нижней части окна сообщения явные признаки угрозы террористического характера отсутствуют

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 (рис. 3-10);

- 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 (рис. 14), затем кликнуть правой кнопкой мыши на прилагаемый файл и выбрать команду «Сохранить как» (рис. 15).

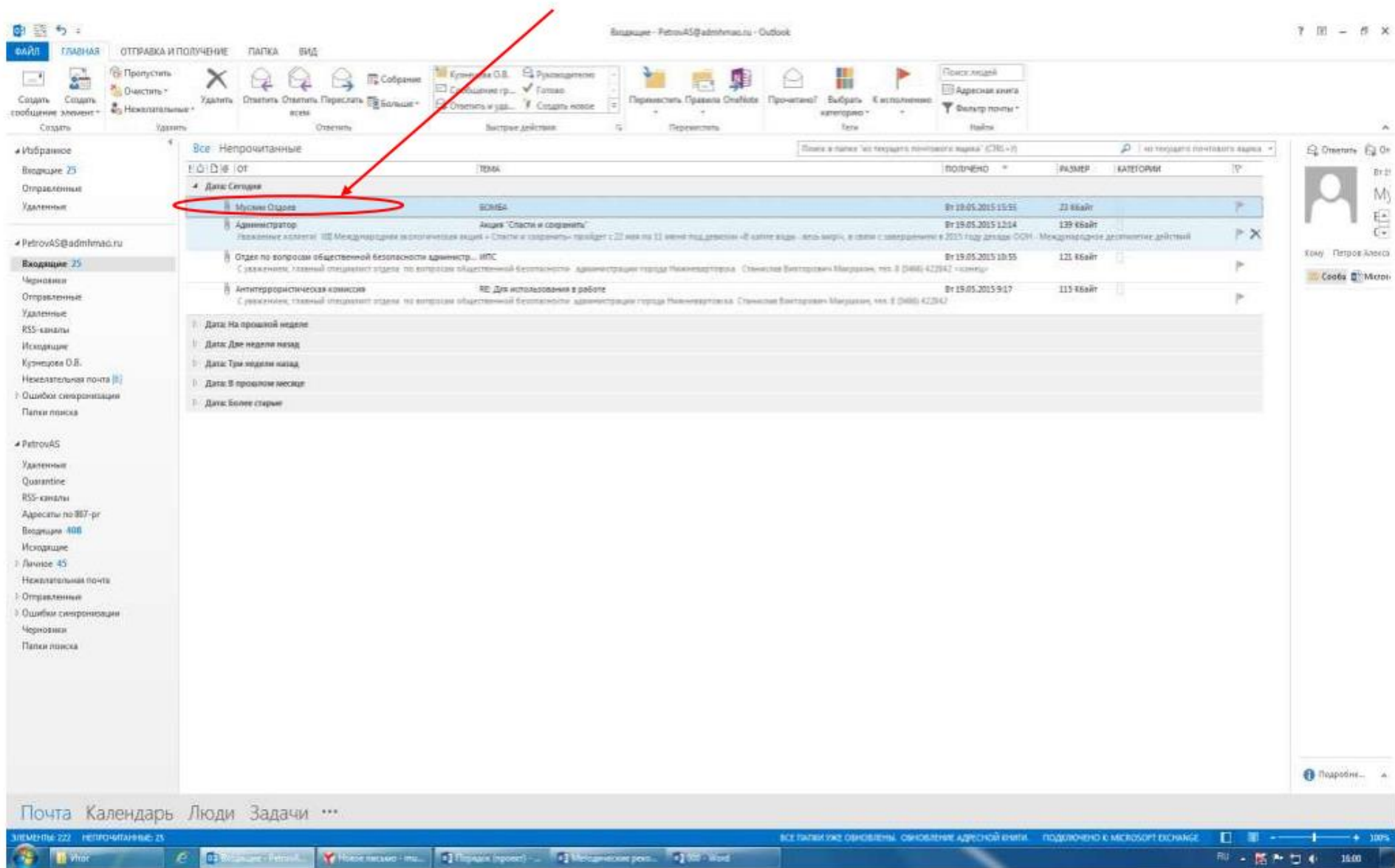


Рис. 14 – Открытие письма, содержащего вложение

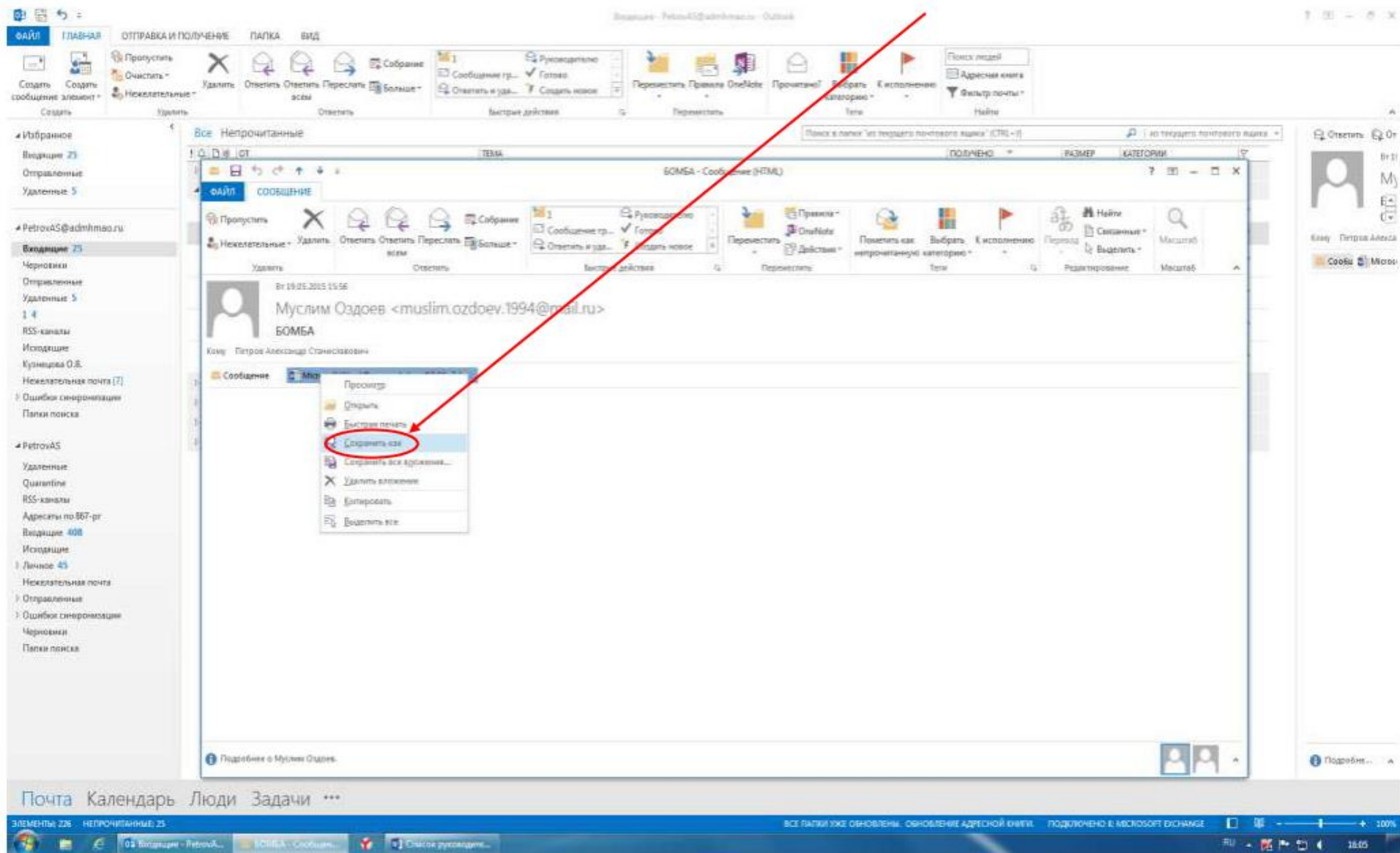


Рис. 15 – Выбор команды «Сохранить как»

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» (рис. 16).

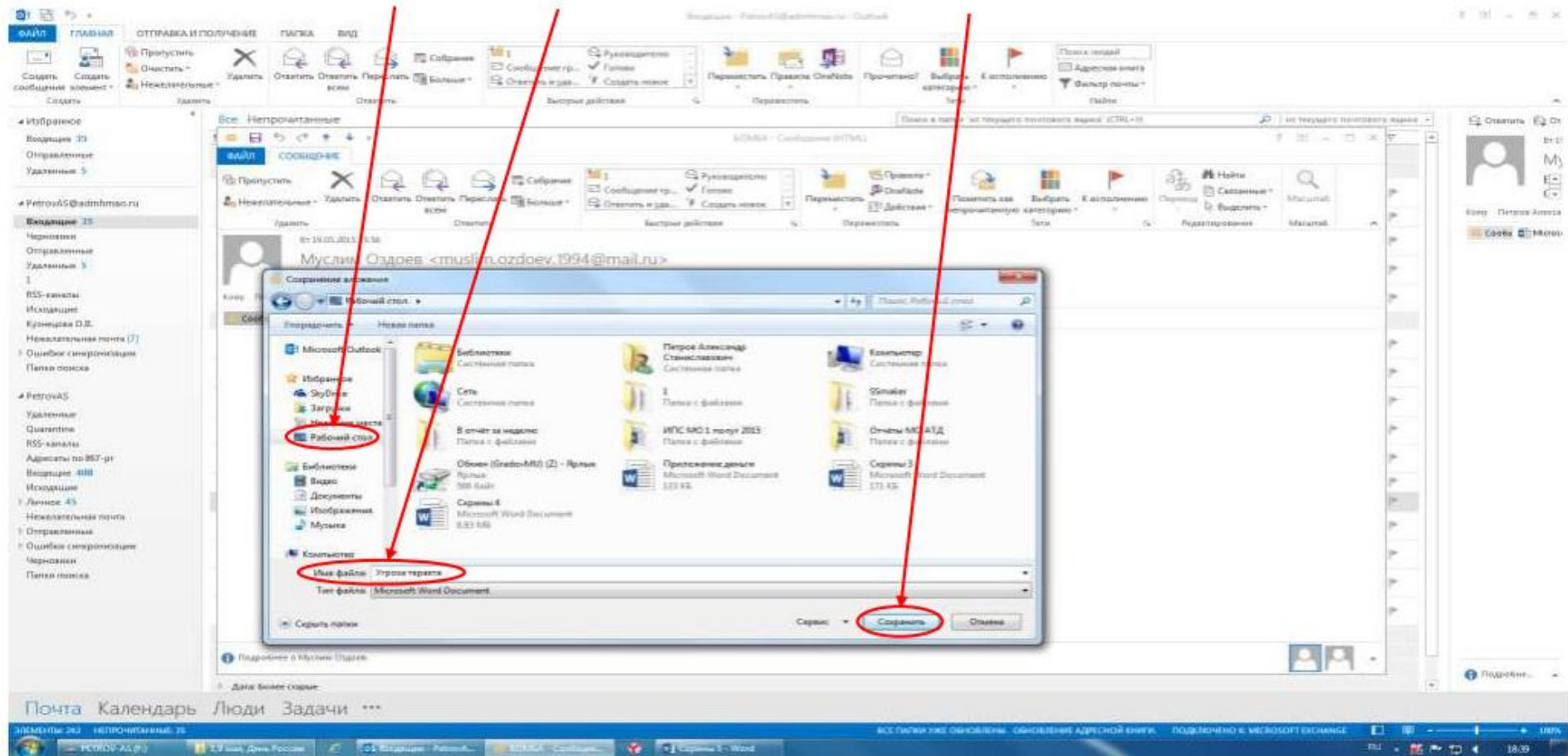


Рис. 16 – Переименование и сохранение документа на рабочий стол

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» (рис. 17), затем свернуть окно электронной почты, выполнить клик правой кнопкой мыши на свободном месте рабочего стола вашего компьютера и выбрать команду «Вставить» (рис. 18).

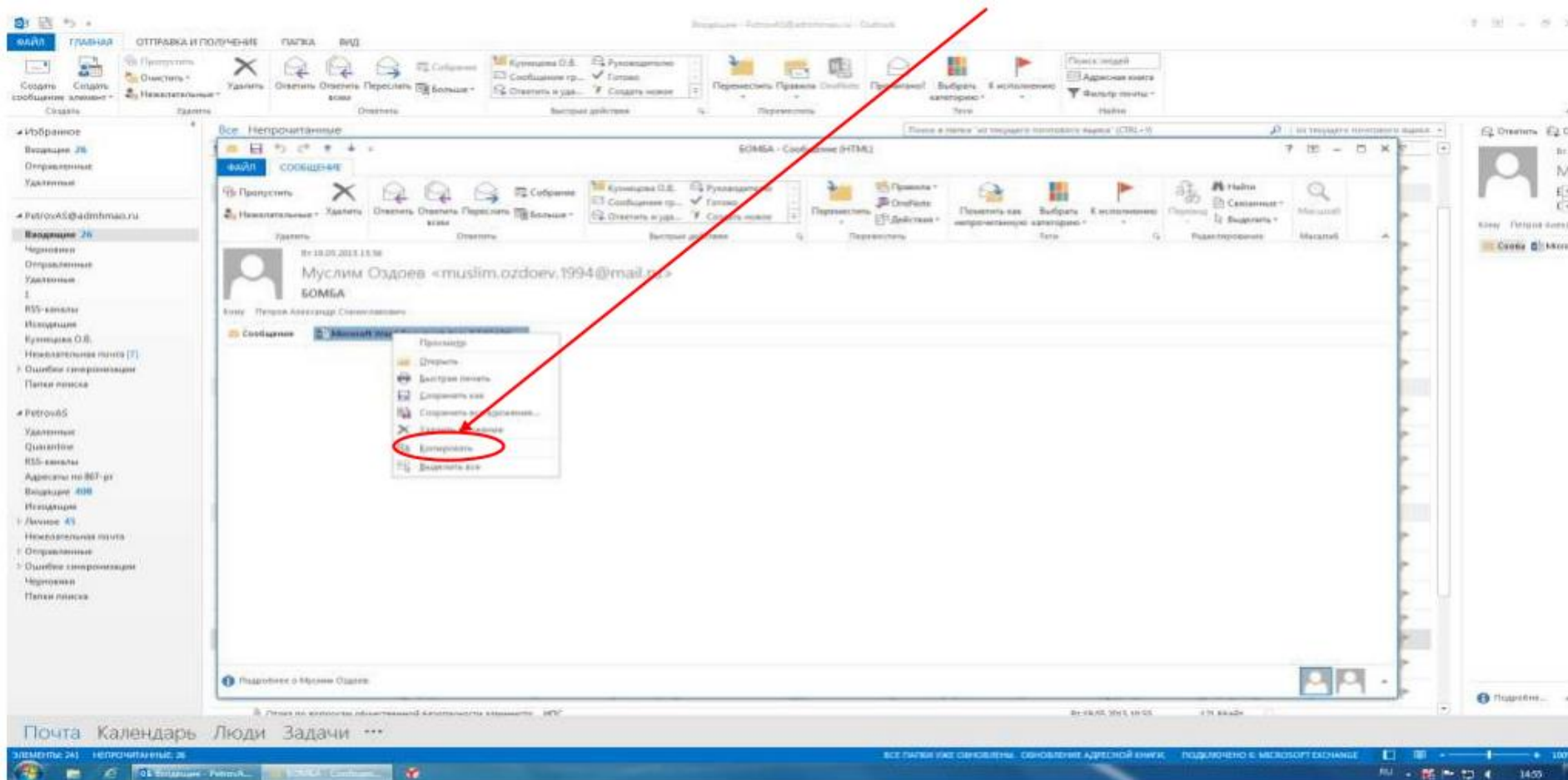


Рис. 17 – Выбор команды «Копировать»

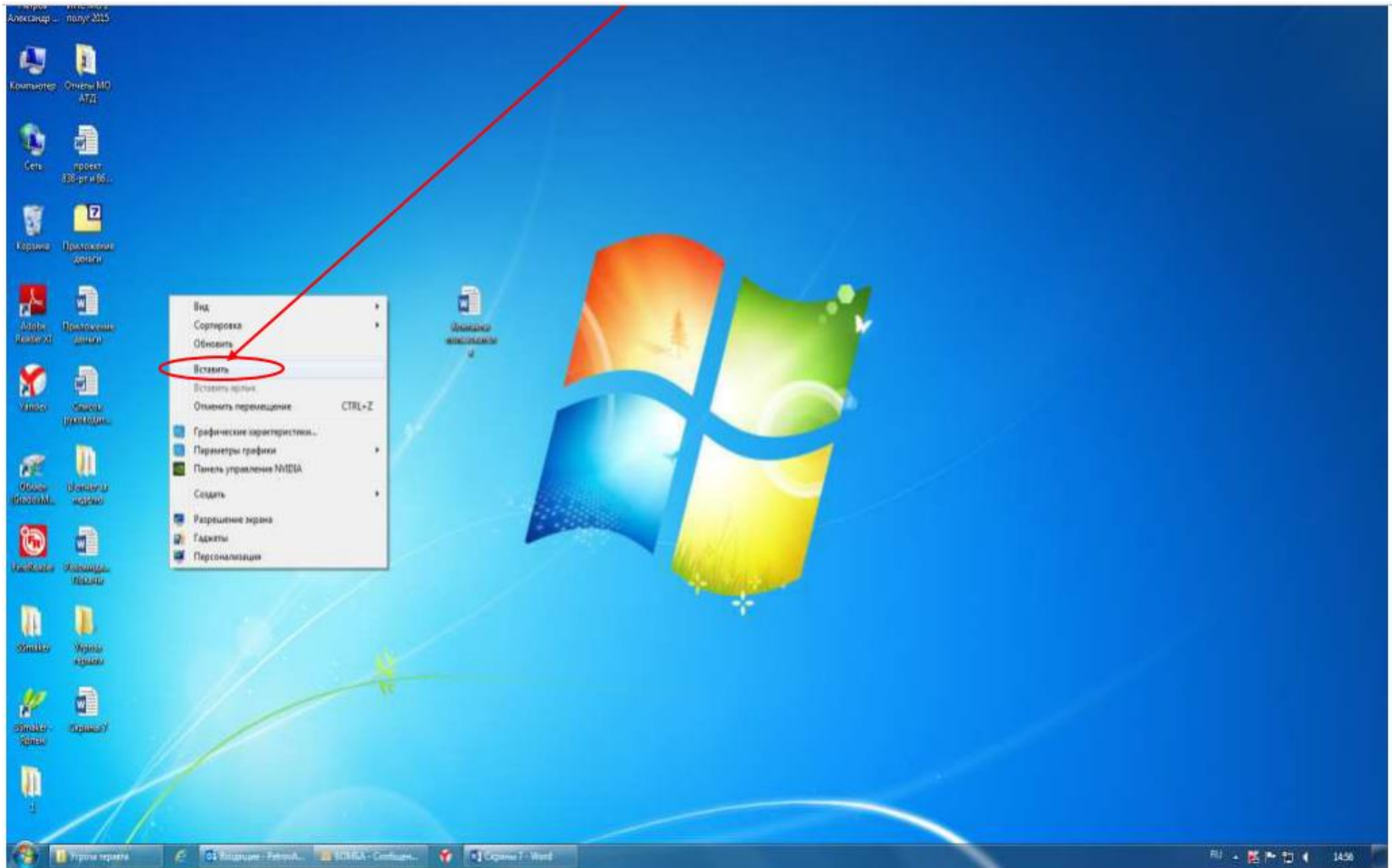


Рис. 18 – Выбор команды «Вставить»

Прилагаемое к письму вложение успешно сохранено на рабочий стол монитора компьютера. Учитывая, что на рабочем столе сохранен 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, сотрудниками организаций в целях обмена электронной корреспонденцией используется электронная почта «MicrosoftOutlook».

В разделах 1 и 2 настоящей Памятки изложен порядок действий сотрудников организаций 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 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», сотрудникам организаций 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).

Раздел 4

Последовательность действий сотрудников организаций 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, сотрудникам организаций необходимо:

- немедленно по телефону проинформировать о поступлении угрозы совершения террористического акта территориальные подразделения МВД России и ФСБ России по месту расположения организации (для Новосибирской области: МВД – 01, ФСБ – 8 (383) 231-05-05);

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

- проинформировать непосредственного руководителя организации;

- 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 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 прибытию 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, сотрудникам организаций **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!**

Учебное издание

Агеенко Людмила Валерьевна

Козарез Ирина Владимировна

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

по противодействию идеологии экстремизма и действиям персонала
и обучающихся ФГБОУ ВО Брянский ГАУ при возникновении угрозы
совершения террористического акта

Редактор Осипова Е.Н.

Подписано к печати 10.10.2022 г. Формат 60x84 ¹/₁₆.

Бумага печатная. Усл. п. л. 2,55. Тираж 40 экз. Изд. №7379.

Издательство Брянский государственный аграрный университет
243365 Брянская обл., Выгоничский район, с. Кокино, Брянский ГАУ