АНТИТЕРРОРИСТИЧЕСКАЯ КОМИССИЯ В СВЕРДЛОВСКОЙ ОБЛАСТИ

ПОРЯДОК ДЕЙСТВИЙ В СЛУЧАЕ ПОСТУПЛЕНИЯ АНОНИМНЫХ СООБЩЕНИЙ ОБ АКТАХ ТЕРРОРИЗМА, В ТОМ ЧИСЛЕ ПОСРЕДСТВОМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ «ИНТЕРНЕТ»

(методические рекомендации)

г. Екатеринбург

2022

Настоящие методические рекомендации разработаны аппаратом антитеррористической комиссии в Свердловской области и предназначены в первую очередь для использования в практической деятельности руководителями объектов (территорий), к антитеррористической защите которых нормативными правовыми актами Правительства Российской Федерации установлены самостоятельные требования. Также использование настоящих методических рекомендаций возможно при проведении мероприятий, связанных с последствиями поступления анонимных сообщений об актах терроризма, в том числе посредством информационно-телекоммуникационной сети «Интернет», руководителями любых предприятий и организаций.

Федеральный закон от 6 марта 2006 года № 35-ФЗ «О противодействии терроризму» является основным источником национального антитеррористического законодательства и нормативным правовым актом федерального уровня, который закрепляет одной из форм противодействия терроризму деятельность субъектов профилактики по предупреждению терроризма, в том числе по выявлению и последующему устранению причин и условий, способствующих совершению террористических актов (профилактика терроризма) (подпункт «а» часть 4 статьи 3), поскольку в современном понятии терроризма в качестве его основных признаков закреплены, во-первых, цель – воздействие на принятие решения органами государственной власти, органами местного самоуправления или международными организациями и, во-вторых, способы достижения этой цели – устрашение населения и (или) иные формы противоправных насильственных действий.

Противодействие терроризму – это деятельность органов государственной власти и органов местного самоуправления, которая реализуется в следующих направлениях: профилактика терроризма, борьба с терроризмом, а также минимизация и (или) ликвидация последствий проявлений терроризма.

При поступлении анонимных сообщений об актах терроризма на телефонные номера и адреса электронной почты предприятий и организаций, работникам организаций необходимо незамедлительно информировать об этом с помощью любых доступных средств связи руководителей организации для реализации неотложных мер по действиям работников и посетителей объекта (территории), а также территориальные органы Федеральной службы безопасности Российской Федерации (далее – ФСБ), Федеральной службы войск национальной гвардии Российской Федерации (далее – Росгвардия), Министерства внутренних дел Российской Федерации (далее – МВД) и Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий (далее – МЧС) по месту нахождения объекта с целью проведения неотложных поисковых и оперативно-розыскных мероприятий.

При направлении указанной информации лицо, передающее информацию с помощью средств связи, сообщает:

– свои фамилию, имя, отчество (при наличии) и занимаемую должность;

– наименование объекта (территории) и его точный адрес;

– дату и время получения информации об угрозе совершения или о совершении террористического акта на объекте (территории);

– характер информации об угрозе совершения террористического акта или характер совершенного террористического акта;

– количество находящихся на объекте (территории) людей;

– имеющиеся достоверные сведения о нарушителе и предпринимаемых им действиях;

– другие значимые сведения по запросу территориального органа ФСБ, Росгвардии, МВД и МЧС.

В случае поступления анонимного сообщения по телефону о заложенных взрывных устройствах при ведении разговора рекомендуется:

1) быть спокойным, вежливым и внимательным, не перебивать звонящего, проявить гибкость, выдержку, терпение, подавлять неприязнь, не реагировать на возможные оскорбления;

2) в процессе разговора отметить возможный возраст, пол, обратить внимание на характерные особенности речи: голос (громкий, тихий, низкий, высокий), темп речи (быстрый, медленный), манеру речи (с издевкой, развязная, нецензурные выражения), произношение (отчетливое, искаженное, с заиканием, шепелявое, акцент, диалект);

3) обязательно отметить звуковой фон (шум машины, транспорта, звук аппаратуры, голоса и т.д.);

4) зафиксировать время начала и конца разговора;

5) в ходе разговора постараться получить информацию: куда, кому, по какому телефону звонит этот человек, какие требования он выдвигает, на каких условиях он согласен отказаться от задуманного, как и когда с ним можно связаться, кому вы можете или должны сообщить об этом звонке;

6) если возможно, еще в процессе разговора сообщить о нем руководству объекта, если нет – немедленно по его окончании;

7) не распространяться о факте разговора и его содержании, максимально ограничить число людей, владеющих информацией;

8) при наличии в телефоне функции автоматического определителя номера записать определившийся номер телефона в тетрадь, что позволит избежать его случайной утраты;

9) при использовании звукозаписывающей аппаратуры сразу же извлечь кассету (диск) с записью разговора и принять меры к его сохранению.

При получении устных угроз непосредственно от человека и невозможности его задержать – зафиксировать время сообщения, запомнить внешние признаки.

При получении информации в виде письма (в бумажном виде) прочитать текст, как можно меньше касаясь документа руками, чтобы не оставлять на нем отпечатков пальцев, вложить его в полиэтиленовый пакет и впоследствии передать прибывшим специалистам правоохранительных органов.

При получении массовой рассылки анонимных сообщений с угрозами совершения террористического акта на адреса электронной почты организаций – не удалять сообщение, зафиксировать время получения, адрес почты, с которой пришло письмо, распечатать его, обеспечить ограничение допуска посторонних лиц к носителю информации.

Ответственный за объект либо лицо его замещающее при поступлении

информации о готовящихся взрывах или заложенных взрывных устройствах в соответствии ранее разработанными в организации организационно-распорядительными документами, обязан:

1) осуществить контроль за незамедлительным доведением имеющейся информации об угрозе или совершении террористического акта в полном объеме до правоохранительных органов;

2) отдать распоряжения об ограничении доступа посторонних лиц на объект;

3) обеспечить усиление охраны объекта и прилегающей территории;

4) оценить реальность угрозы совершения террористического акта (опросить охрану объекта, сотрудников и посетителей (обучаемых) на предмет обнаружения посторонних предметов и подозрительных лиц);

5) обеспечить просмотр имеющихся записей за предыдущие сутки на предмет выявления проникновения подозрительных лиц или проноса вещей и предметов в помещения и на территорию объекта;

6) при получении достаточных данных о реальности угрозы совершения террористического акта организовать немедленную эвакуацию сотрудников и иных лиц с территории объекта, обратив их внимание на необходимость обеспечения максимального соответствия одежды погодным условиям;

7) эвакуацию производить в заблаговременно определенный пункт временного размещения эвакуированных лиц на удаленном от объекта расстоянии с последующим ожиданием прибытия сотрудников правоохранительных органов;

8) принять меры по недопущению паники;

9) обязать всех подчиненных лиц незамедлительно докладывать об обнаружении подозрительных лиц или предметов;

10) организовать постоянный мониторинг при помощи систем видеонаблюдения с целью выявления подозрительных лиц или вещей и предметов в помещениях и на территории объекта;

11) обеспечить условия для правоохранительных органов, МЧС, организаций здравоохранения для проведения мероприятий по предотвращению, локализации и ликвидации угрозы взрыва;

12) по прибытии правоохранительных органов доложить обстановку, предоставить всю необходимую информацию (наименование организации, юридический и фактический адрес объекта, количество работников и посетителей, находящихся в здании, проведена ли эвакуация и, если проведена частично, то сколько еще граждан остается в здании, есть ли обнаруженные подозрительные предметы, кто из представителей правоохранительных органов уже находится на объекте), действовать по указаниям правоохранительных органов;

13) прибывшим сотрудникам правоохранительных органов предоставить план здания, техническую документацию объекта с поэтажными схемами и выделить проводника из числа наиболее подготовленных сотрудников, владеющих сведениями о планировке территории объекта;

14) не распространять в СМИ сведения о данных сообщениях и действиях сотрудников правоохранительных органов до окончания мероприятий.

Оповещение людей, находящихся на объекте (территории), осуществляется с помощью технических средств (циркулярной связи, автоматических систем

оповещения и телефонной связи), которые должны обеспечить:

– подачу звуковых и (или) световых сигналов в здания и помещения, на участки территории объекта с постоянным или временным пребыванием людей;

– трансляцию речевой информации о характере опасности, необходимости и путях эвакуации, других действиях, направленных на обеспечение безопасности.

Эвакуация людей по сигналам оповещения должна сопровождаться:

– включением аварийного освещения;

– передачей специально разработанных текстов, направленных на предотвращение паники и других явлений, усложняющих процесс эвакуации (скопления людей в проходах, тамбурах, на лестничных маршах и других местах);

– включением световых указателей направлений и путей эвакуации;

– открыванием дверей дополнительных эвакуационных выходов (например, оборудованных электромагнитными замками).

Сигналы оповещения при угрозе совершения или совершении террористического акта должны отличаться от сигналов другого назначения. Количество оповещателей, их мощность должны обеспечить необходимую слышимость во всех местах постоянного или временного пребывания людей.

К примеру: «Внимание всех!!! Террористическая угроза. Всем покинуть здание учреждения. Сохраняйте спокойствие».

На территории объектов следует применять рупорные громкоговорители, которые могут устанавливаться на опорах освещения, стенах зданий и других конструкциях. Оповещатели не должны иметь регуляторов громкости и разъемных соединений. Коммуникации систем оповещения в отдельных случаях допускается проектировать совмещенными с радиотрансляционной сетью объекта. Управление системой оповещения должно осуществляться из помещения охраны, диспетчерской или другого специального помещения.

При отсутствии телефонной связи или ее повреждении следует предусмотреть систему посыльных, в качестве которых можно использовать работников учреждения (организации).

Возможно использование при осуществлении оповещения SMS-рассылки об эвакуации.

При обнаружении взрывоопасного предмета (либо с признаками таковых) запрещается:

1) дотрагиваться до взрывоопасного предмета и перемещать его;

2) заливать предмет жидкостями, засыпать грунтом, накрывать каким-либо материалом;

3) пользоваться радиоаппаратурой и средствами мобильной связи вблизи данного предмета;

4) оказывать на предмет до его обезвреживания температурное, звуковое, механическое и электромагнитное воздействие.

При принятии решения об эвакуации сотрудников и персонала руководителем объекта необходимо при наличии возможности и ранее предварительно определенного алгоритма взаимодействия уточнить установление сотрудниками ФСБ факта массовой рассылки на территории Российской Федерации анонимных сообщений, поступающих с использованием средств

анонимизации через IP-телефонию или по каналам электронной почты.

Дополнительно при поступлении анонимных сообщений об угрозе террористического акта на электронные почтовые ящики необходимо сразу перенаправлять анонимные сообщения в формате «.eml» на почтовый ящик УФСБ «antispam-66@yandex.ru».

Инструкция по выгрузке электронных сообщений в формате EML

Почтовый web-сервис «Mail.ru».

1. Открыть сообщение.
2. Выбрать раздел «Ещё» → «Скачать на компьютер». Письмо сохранится в формате EML.

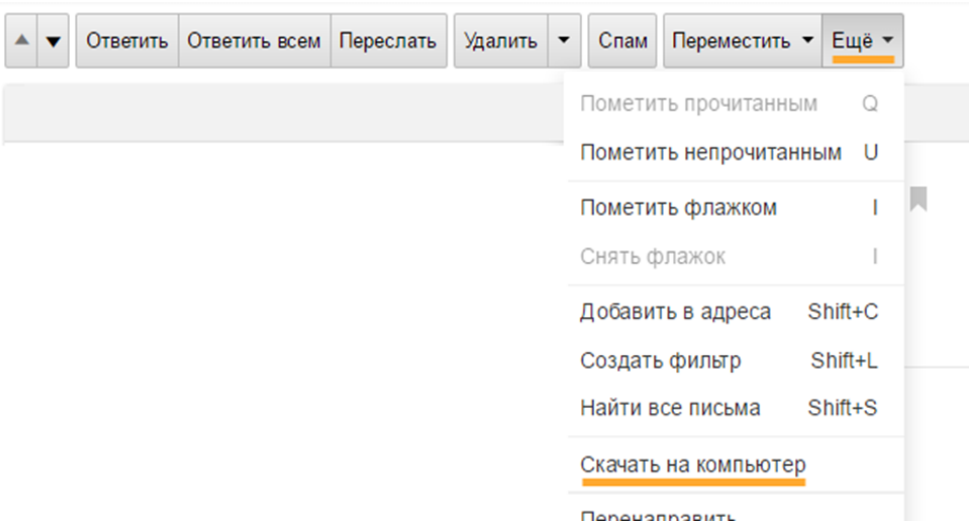

Рисунок 1.

Почтовый web-сервис «Яндекс.Почта».

1. Открыть сообщение.

2. Выбрать раздел, обозначенный кнопкой: ••• . Далее выбрать «Свойства письма». В новой вкладке откроется исходный код письма.

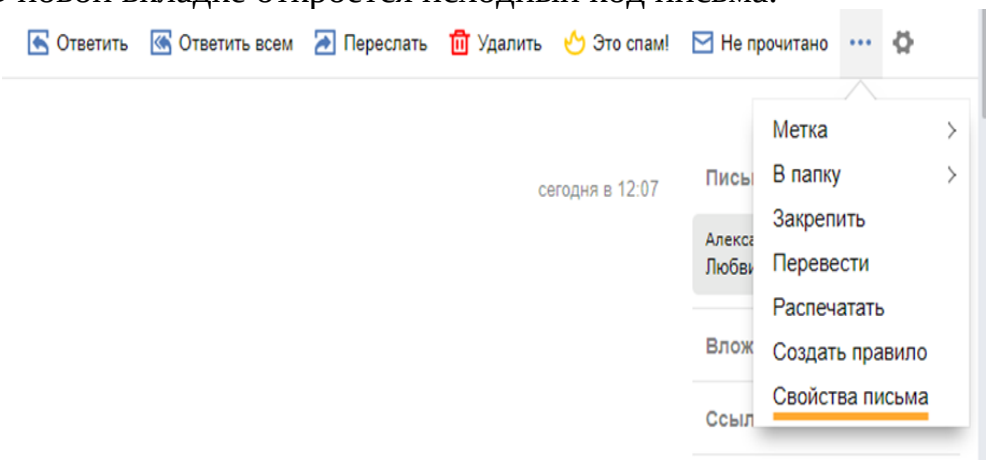

Рисунок 2.

3. Нажать правой кнопкой мыши в любом месте страницы, затем – «Сохранить как…».

4. Нажать «Сохранить». Письмо сохранится в формате EML.

Почтовый web-сервис «Gmail».

1. Открыть письмо.

2. Нажать кнопку, обозначенную иконкой: . Выбрать пункт «Показать оригинал». В новой вкладке откроется исходный код письма.

3. Нажмите «Скачать оригинал». Письмо сохранится в формате EML.

Почтовый web-сервис «Рамблер/Почта».

1. Открыть письмо.

2. Нажать кнопку, обозначенную иконкой:  . В новой вкладке откроется исходный код письма.

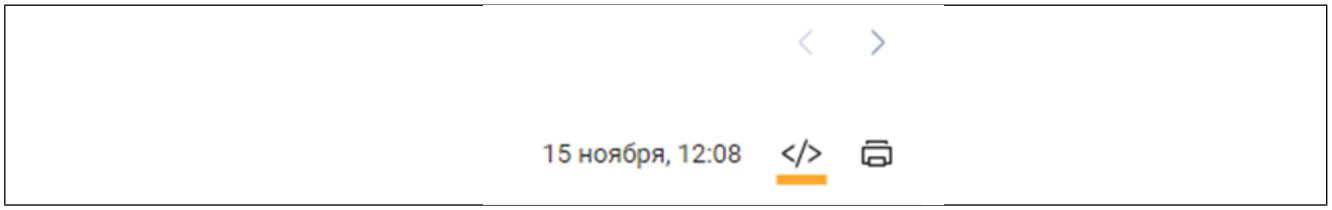

Рисунок 3.

3. Нажать правой кнопкой мыши в любом месте страницы, затем – «Сохранить как…».

4. Нажать «Сохранить».

5. Переименовать расширение файла в .eml.

Почтовый windows-клиент Microsoft Outlook 2013/2016/2019.

1. Открыть письмо.

2. В верхней части окна с сообщением нажать кнопку «Больше», «Переслать как вложение».

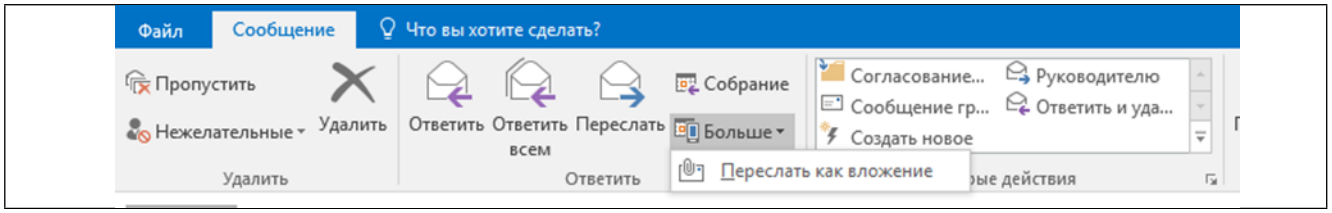

Рисунок 4.

3. Откроется проект нового электронного сообщения.

4. Переслать данное сообщение на web-сервис «Яндекс.Почта».

5. Открыть сообщение в web-сервис «Яндекс.Почта».

6. Сохранить вложение в формате .eml.

Почтовый windows/linux-клиент Mozilla Thunderbird.

1. Выбрать письмо, нажать правую кнопку мыши.

2. Выбрать пункт «Переслать как», «Вложение».

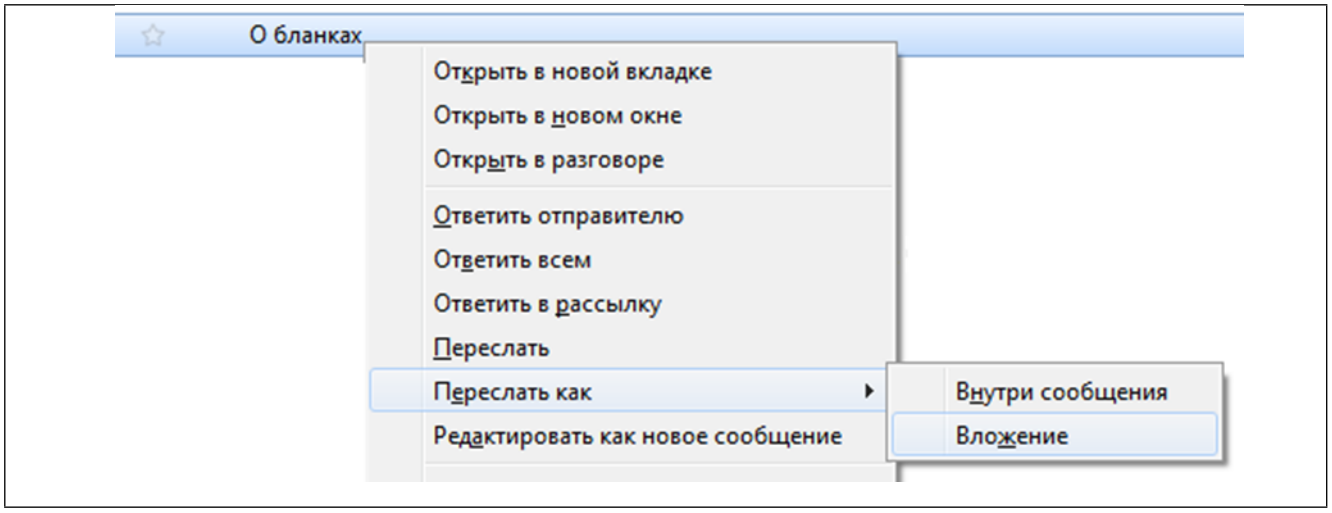

Рисунок 5.

3. Откроется проект нового электронного сообщения.

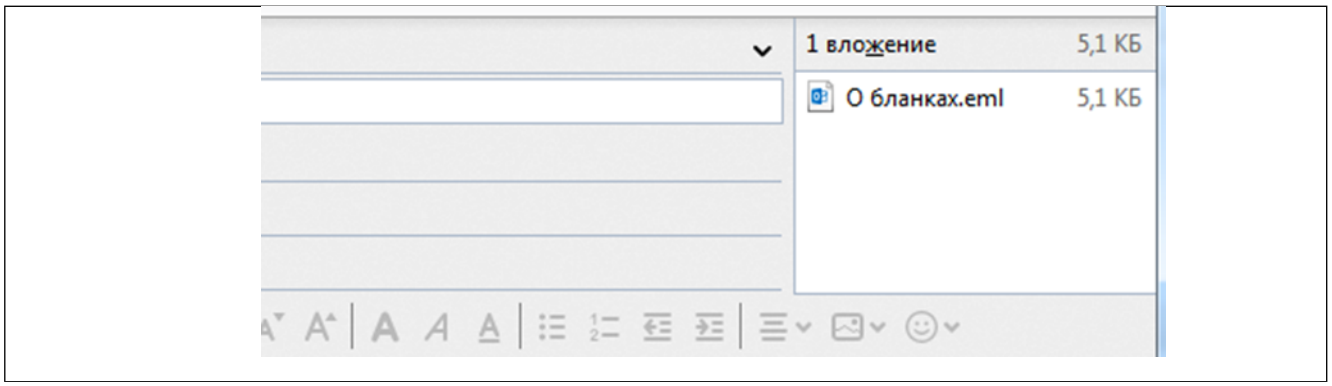

Рисунок 6.

4. Сохранить вложение в формате .eml.