Приложение 1
к приказу от 15.02.2022г. № 17-А

Инструкция
по действиям персонала ГБУ РК «Реабилитационный центр»
при угрозе совершения террористического акта

Настоящая Инструкция по действиям персонала ГБУ РК «Реабилитационный центр» при угрозе совершения террористического акта (далее – Инструкция) разработана в целях обеспечения антитеррористической безопасности объекта с массовым пребыванием людей и устанавливает порядок действия руководителя и персонала ГБУ РК «Реабилитационный центр» (далее - Учреждение) при возникновении угрозы совершения террористического акта и взаимодействия с территориальными органами безопасности, территориальными органами Министерства внутренних дел Российской Федерации (далее - правоохранительные органы).

Весь персонал Учреждения, независимо от занимаемой должности, обязан четко знать и строго выполнять установленный порядок действий при угрозе совершения террористического акта и не допускать действий, которые могут вызвать угрозу жизни и здоровью получателей социальных услуг, родителей/законных представителей получателей социальных услуг, работников Учреждения, посетителей,

1. Действия работников Учреждения в случае обнаружения подозрительного предмета, который может оказаться взрывным устройством.

Подозрительные предметы могут быть обнаружены около входа в Учреждение, в коридорах, на лестничных площадках, вблизи дверей кабинетов работников, а также в местах общего пользования.

Внешний вид предмета может скрывать его настоящее назначение. В качестве камуфляжа для взрывных устройств используются обычные бытовые предметы: сумки, пакеты, свертки, коробки, игрушки и т. п.

При обнаружении подозрительного предмета работнику, обнаружившему подозрительный предмет, необходимо незамедлительно сообщить о случившемся непосредственному руководителю, ответственному лицу за организацию работы по обеспечению антитеррористической защищённости в ГБУ РК «Реабилитационный центр», а в случае его отсутствия - директору или заместителю директора Учреждения.

Ответственное лицо за организацию работы по обеспечению антитеррористической защищённости в ГБУ РК «Реабилитационный центр», а в его отсутствие администрация Учреждения, обязан немедленно сообщить (отдать указание о немедленном информировании) об обнаружении подозрительного предмета:

- в дежурную часть Отдел МВД России по г. Евпатории, дежурная часть: +7 (36569) 9-06-90, +7 (36569) 9-06-91, +7 (36569) 9-06-93, +7 (999) 461-02-78 или 102;
- в единую спасательную службу по телефону - 112.

При обнаружении подозрительного предмета нельзя предпринимать самостоятельно никаких действий с находками или подозрительными предметами, которые могут оказаться взрывными устройствами, поскольку это может привести к их взрыву, многочисленным жертвам и разрушениям.

До прибытия оперативно-следственной группы руководителю/заместителю руководителя Учреждения необходимо:

1) дать указание получателям социальных услуг, их законным представителям, работникам Учреждения и посетителям находиться на безопасном расстоянии от обнаруженного подозрительного предмета;

2) опросить людей, находящихся рядом;

3) постараться установить, чья вещь и кто мог ее оставить;

4) закрыть помещения, в которых находятся материальные ценности и документы, в случае необходимости принять меры к их эвакуации;

5) в случае необходимости приступить к эвакуации людей согласно имеющемуся плану, расположенному в коридорах Учреждения;

6) обеспечить возможность беспрепятственного доступа к месту обнаружения подозрительного предмета автомашин и сотрудников правоохранительных органов, скорой медицинской помощи, пожарной охраны, спасательных служб, служб эксплуатации;

7) обеспечить присутствие лиц, обнаруживших находку, до прибытия оперативно-следственной группы и фиксацию их установочных данных;

8) получив информацию о возможности возобновления дальнейшей работы Учреждения, продолжить выполнять свои должностные обязанности.

Во всех случаях нельзя трогать, передвигать, вскрывать обнаруженный подозрительный предмет.

Кроме того, необходимо:

1) зафиксировать время обнаружения подозрительного предмета;

2) сделать все возможное, чтобы люди отошли как можно дальше от находки;

3) дождаться прибытия оперативно - следственной группы.

По прибытии сотрудников правоохранительных органов действовать по их указанию.

2. Действия работников Учреждения в случае поступления сообщения об угрозе совершения террористического акта по телефону.

В настоящее время телефон является основным каналом поступления сообщений, содержащих информацию о заложенных взрывных устройствах, о захвате людей в заложники, вымогательстве и шантаже.

Звонок с угрозами может поступить в адрес любого работника.

Работник Учреждения, на чей номер служебного телефона поступил звонок с угрозой совершения террористического акта, не должен оставлять его без внимания и обязан незамедлительно обеспечить своевременную передачу полученной информации руководителям Учреждения.

Руководители Учреждения обязаны незамедлительно сообщить о поступившем звонке с угрозой в правоохранительные органы по телефонам, указанным в пункте 1 настоящей Инструкции.

Значительную помощь правоохранительным органам при проведении оперативно-розыскных мероприятий по данным фактам окажут следующие действия предупредительного характера.

Работник Учреждения, на чей номер служебного телефона поступил звонок с угрозой совершения террористического акта, должен:

1) постараться дословно запомнить разговор и зафиксировать его на бумаге;

2) по ходу разговора отметить пол, возраст звонившего и особенности его речи;

3) обязательно отметить звуковой фон (шум автомашин или железнодорожного транспорта, звук теле- или радиоаппаратуры, посторонние голоса и другое);

4) обязательно зафиксировать точное время начала разговора и его продолжительность;

5) если возможно, еще в процессе разговора сообщить о нем руководителю Учреждения;

6) не распространять сведения о факте разговора и его содержании, максимально ограничить число людей, владеющих данной информацией.

До прибытия сотрудников правоохранительных органов исключить доступ посторонних лиц на территорию объекта.

По прибытии сотрудников правоохранительных органов действовать по их указанию.

Ответственному лицу за организацию работы по обеспечению антитеррористической защищённости в ГБУ РК «Реабилитационный центр» необходимо регулярно со всеми работниками Учреждения проводить инструктаж о порядке действия при приеме телефонных сообщений с угрозами террористического характера.

3. Действия работников Учреждения в случае поступления угрозы в письменной форме.

Угрозы в письменной форме могут поступить в Учреждение как по почте, так и в

Работник Учреждения, на которого возложены обязанности по принятию поступающей в Учреждение корреспонденции, обязан сообщить о поступившей угрозе в письменной форме руководителям Учреждения, которые в свою очередь обязаны принять меры к сохранению и своевременной передаче в правоохранительные органы полученных материалов.

После получения материала угрожающего характера необходимо обращаться с ним максимально осторожно:

1) по возможности убрать его в чистый, плотно закрываемый полиэтиленовый пакет и поместить в плотную папку;

2) постараться не оставлять на нем отпечатков своих пальцев;

3) если документ поступил в конверте, его вскрытие произвести только с левой или правой стороны, аккуратно отрезая кромки ножницами;

4) сохранить все: сам документ с текстом, любые вложения, конверт и упаковку - ничего не выбрасывать;

5) не расширять круг лиц, знакомившихся с содержанием документа;

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

При проставлении на сопроводительных документах резолюций и других надписей на самих анонимных материалах не должно оставаться следов.

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

4. Действия работников Учреждения в случае захвата заложников.

При захвате людей в заложники необходимо:

1) о сложившейся ситуации незамедлительно сообщить в правоохранительные органы;

2) не вступать в переговоры с террористами по собственной инициативе;

3) принять меры к беспрепятственному проходу (проезду) на объект сотрудников правоохранительных органов, спасательных служб, автомашин медицинской помощи;

4) по прибытии сотрудников спецподразделений ФСБ России и МВД России оказать им помощь в получении интересующей их информации;

5) при необходимости выполнять требования преступников, если это не связано с причинением ущерба жизни и здоровью людей, не противоречить преступникам, не рисковать жизнью окружающих и своей собственной;

6) не допускать действий, которые могут спровоцировать нападавших к применению оружия и привести к человеческим жертвам.

Во время проведения спецслужбами операции по освобождению заложников необходимо неукоснительно соблюдать следующие требования:

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) при возможности, держаться подальше от проемов дверей и окон.

5. Действия работников при открытом получении информации об угрозе совершения преступления террористического характера

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

отправителе сообщения. Также в верхней части окна сообщения отображена дата отправления сообщения, имя и электронный адрес отправителя.

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 вверхнем 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 сообщениясс 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.

6. Действия работников 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» частоприлагается какой-либо файл (документ, фотографии, видео и т.п.). Приложенный к письму файл называется вложением. Письма, содержащие вложение, подразделяются на 2 вида:

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

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

Во всех вышеприведённых примерах получения по электронной почте писем с вложениями (пункты 6.1 и 6.2 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 5;

- сохранить прилагаемое к письму вложение (документ, аудиофайл, фотографию, видео и т.п.) на рабочий стол монитора или другое место на жесткомдиске 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 мышина 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 невыбрать 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 мышина 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 действияс поступившими материалами кроме их копирования и сохранения.

7. Действия работников при получении информации об угрозе совершения преступления террористического характера, поступившей по электроннойпочте 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 и работниками Учреждений в целях обмена электронной корреспонденцией используется электронная почта «MicrosoftOutlook». В разделах 5 и 6 настоящей Памятки изложен порядок действий должностных лиц и работников 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

ящиках» примерно одинаковый. Соответственно,независимо от вида электронной почты, на любой компьютер пользователя (работника или 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», работникам учреждений необходимо выполнить порядок действий, предусмотренный разделами 6, 7 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 или организации), обслуживающую работуофисной техники и информационно-телекоммуникационной сети Интернет, обеспечив при этом наименьшую осведомлённость посторонних лиц о поступлении информации об угрозе террористического характера.

8. Последовательность действий должностных лиц и работников Учреждений при получении информации об угрозе совершения преступления террористического характера, поступившей посредством электронных почтовых сервисов международнойинформационно-коммуникационной сети Интернет.

8.1. При получении по электронной почте сообщений, содержащих угрозы террористического характера необходимо:

- проинформировать непосредственного руководителя 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 Инструкцией;
- принять меры, ограничивающие доступ посторонних лиц к рабочемуместу 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 Отдел МВД России по г. Евпатории 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.

8.2. При получении по электронной почте сообщений, содержащих угрозы террористического характера, должностным лицам и работникам учреждений **ЗАПРЕЩАЕТСЯ**:

- перемещать из папки «Входящие» и (или) удалять поступившие поэлектронной почте сообщения об угрозе теракта;
- расширять круг лиц, ознакомившихся с содержанием поступившегосообщения;
- отвечать на поступившее сообщение отправителю (адресату) письмас 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.