Тимощук А.С.,

доктор философских наук, доцент
Владимирский юридический институт ФСИН России

Трофимова Н.Н.,

кандидат юридических наук, доцент
Владимирский юридический институт ФСИН России

Оперативно-технические аспекты противодействия ложному минированию

Преднамеренный ложный вызов является разновидность террористической атаки. Статья посвящена проблеме противодействия терроризму в социотехнической среде. Общественное сознание, опосредованное техносферой, уязвимо не только из-за самих терактов, но и вследствие скоординированных ложных вызовов экстренных служб. Авторы исходят из позиции, что схема реагирования на поступающие угрозы нуждается в оптимизации, так как целью «телефонных» террористов является воздействие на общественное сознание через нарушение функциональности социальной системы, распространение слухов и паники.

Организованные массовые фейк-вызовы экстренных служб являются новеллой в обеспечении государственной и общественной безопасности. В случае получения тревожного вызова Дежурные службы МВД, МЧС и ФСБ принимают меры экстренного реагирования в рамках совместных приказов по организации взаимодействия. По существующей схеме они обязаны прибыть на место для отработки сигнала, даже если он фиктивный. В зависимости от уровня угроз и объекта атаки помимо экстренных служб могут приехать представители прокуратуры и следственного комитета, скорая помощь; задействоваться спецтехника. Такими ложными сообщениями наносится удар не только по системе безопасности и государственного управления, но и по экономике. Перегрузка систем экстренного реагирования безрезультатными сигналами означает, что те, кто реально нуждается в помощи, может ее не получить. Функциональные отказы вместе со слухами, паникой и недовольством – вот еще одно последствие необоснованных вызовов. Таким образом, скоординированные заведомо ложные вызовы – это разновидность террористических актов, которые, несмотря на отсутствие жертв, дорого обходятся обществу и государству.

В условиях конкурентной борьбы между странами ложные вызовы о минировании могут осуществляться в рамках кампании по дестабилизации социально-политической обстановки в государстве-мишени его соперниками под прикрытием. Тема осложняется еще и тем, что субъектами террористических угроз могут выступать очень разные личности: террорист, социальный активист, мститель, хулиган, самоубийца, психически больной[1].

Не классифицирован тип организованной группы телефонных террористов, оказывающих услуги заинтересованным государствам в условиях информационной войны и точечным управлением страхом. Это могут быть центры частных военных компаний, специализирующихся по передаче ложной информации, а также формирования международных террористических групп. Распределение ложных сообщений по времени и пространству свидетельствует о едином командовании акции, что означает, что расследование подобных случаев – прерогатива оперативной разведки, нежели управления по противодействию экстремизму и терроризму МВД.

Трудно также провести границу между телефонным террористом, хакером, кибердиверсантом, сотрудником секретных служб, т.к. перечень компетенций этих видов деятельности во многом пересекается и заключается в ведении ненасильственной войны: 1) мониторинг медийной активности;

[1] Тактика общения с «телефонными террористами»: проблемы документирования, проведения экспертизы, ведения переговоров : практическое пособие. М. : ИМЦ ГУК МВД России, 2001. 36 с.

2) проведение психологических операций; 3) вброс фейков; 4) использование прокси-инструментов для имитации субъекта[1].

Результативность телефонного терроризма заключается в реализации множества задач недорогими действиями, которые требуют минимум специальной технической подготовки (например, в случае реальной закладки взрывчатых веществ и осуществлении терактов). Злоумышленники достигают целого ряда эффектов: 1) дезориентация органов правопорядка и спецслужб; 2) отвлечение внимания полиции от реальных происшествий и террористических атак; 3) перегрузка силовых ведомств и экстренных служб; 4) дезорганизация работы муниципальных учреждений; 5) усыпление бдительности перед реальной угрозой; 6) материальный ущерб; 7) демонстрация протеста; 8) вселение страха и создание очагов паники; 9) срыв планового предоставления медицинской помощи. Из-за неразберихи во время эвакуации пациенты могут умереть, так как им вовремя не будет оказана помощь.

Можно говорить о высоком профессионализме телефонных атак, поскольку изощренность методов совершения преступления не оставляет шансов на его раскрытие стандартными методами. Криминальная эффективность в данном случае достигается следующими средствами: 1) обеспечением анонимности; 2) достижением цели террористической деятельности; 3) технической изощренностью; 4) низкой себестоимостью услуг телефонного терроризма; 5) нанесением крупного ущерба государству.

При этом механизм эффективного противодействия угрозам телефонного терроризма еще не выработан. Причем если правовое решение существует в виде ст. 207 УК РФ, узким местом является именно оперативно-розыскная эффективность. По мнению экспертов, раскрытие преступления, предусмотренного ст. 207 УК РФ, – это один из наиболее сложных и трудоемких процессов, в котором задействовано большое количество сил и средств различных служб (ФСБ, МВД, МЧС и другие)[2].

Нужны меры по деанонимизации получаемых сообщений: совершенствование фильтрации спама и анонимных сообщений. Необходимо «прикрыть дыры» в уязвимости связи. В этом смысле консервативный подход специалиста по кибербезопасности Е.В. Касперского, выступающего с инициативой паспортизации доступа в Интернет и ограничении информационных прав, выглядит совсем не ретроградным. Обеспечение состояния защищенности личности, общества и государства от внутренних и внешних угроз позволяет говорить о необходимости регулирования права на Интернет. Смена схемы организационной структуры системы противодействия терроризму сразу же позволит сделать ложные вызовы неэффективными.

Еще одним направлением являются аналитика, инсайдерская информация, разработка разведывательных средств обнаружения телефонных террористов, взаимодействие между спецслужбами и правоохранительными органами зарубежных стран. Сейчас страны, через которые поступают ложные сообщения, находятся в противостоянии к нам, они могут отказываться от сотрудничества с российскими компьютерными криминалистами. Если исходить из концепции нарастания эскалации в связи с ограниченностью ресурсов, то государство должно иметь автономные средства идентификации субъекта. Для этого нужны технические решения, позволяющие определить фактического отправителя сообщения.

Следующий вывод касается концептуальных решений о способах реагирования в условиях массированных атак, вызывающих дезорганизацию работы МЧС, МВД, ФСИН, ФСБ и муниципальных учреждений. Действующий алгоритм сфокусирован на том, чтобы принимающий звонок запомнил как можно больше информации о передатчике информации (пол, возраст, особенности речи, звуковой фон, характер звонка, время, продолжительность). После фиксации содержимого поступившей угрозы ответственное лицо информирует руководителя организации и приступает к действиям

[1] Тимощук А.С. Общественное сознание как мишень терроризма // Пенитенциарное право: юридическая теория и правоприменительная практика. 2019. № 2. С. 130-136.

[2] Ганиев Т.Г. К вопросу борьбы с телефонным терроризмом // Современные проблемы права: теория и практика : материалы Всероссийской научно-практической конференции. 2011. С. 192-197.

по эвакуации постоянного и переменного составов.

Для противодействия угрозам ложного минирования, совершаемых дистанционно с зарубежных территорий, необходимо моделировать динамику и структуру такой преступности, личность возможного преступника, поскольку негласные формы работы затруднены; создавать условия, осложняющие совершение подобных удаленных преступлений; вести учет фиктивных информационных ресурсов; улучшать осведомленность оперативников об уловках и схемах, используемых преступниками; повышать квалификацию и заниматься самообразованием в целях прогнозирования следующих террористических атак и способов мало затратного предупреждения и реагирования[1].

В условиях, когда растет число экстремистских угроз, целесообразно выработать иную схему принятия решений в случае поступления террористических угроз, учитывающую возможность ложного вызова, провокации, использующих состояние защищенности для дезорганизации деятельности, создания паники и недовольства. Для того чтобы состоятельно проверить обоснованность угрозы, можно использовать видоизмененную коммуникационную модель Г. Лассуэлла: «Кто говорит? Что говорит? По какому каналу? Кому говорит? С каким эффектом?». При поступлении массовых анонимных угроз через зарубежные каналы координационный штаб по противодействию терроризму может рассматривать их как разновидность атаки «переполнение буфера», ведущей к отказу обслуживания, парализации социальных систем. Эффективность таких атак связана с уязвимостью социотехнической среды, основанной на одновременном соединении важных детерминантов – массовости, кибернетической интеграции и корпоративном комплайенс. Если первые два фактора являются сущностными и неустранимыми для современного постиндустриального технократического общества, то такой атрибут, как стандарт реагирования – это опция, настройки которой зависят от управленцев. Частота анонимных террористических угроз и неполнота информации – достаточные основания для игнорирования входящих сообщений в целях сохранения работоспособного состояния общественной системы, что сопряжено с риском, другим определяющим фактором современной социотехнической среды. Обеспечение функциональности социотехнических систем требует асимметричных решений поступающим террористическим угрозам, например обучению риск-менеджменту и разработке юридически обоснованного риска в принятии решений по противодействию терроризму. Чтобы фатальная опасность не приводила к коллапсу, сама система должна поменять индикаторы устойчивости.

Евтушенко А.А.

Сибирский юридический институт МВД России (г. Красноярск)

Обучение боевым приемам борьбы с использованием технических средств обучения и игрового метода курсантов и слушателей образовательных учреждений МВД России

В последние годы отчетливо выявились проблемы профессиональной подготовки сотрудников органов внутренних дел (далее − ОВД). В ряде случаев морально-психологическая подготовка к действиям в сложных, экстремальных условиях приводит к непредвиденным последствиям.

Служебная деятельность сотрудников полиции в ситуациях пресечений преступлений и правонарушения предъявляет высокие требования к их специальной подготовке. В основном к преступлениям подталкивают социальные причины - пьянство и безработица.

[1] Подшивалов А.П., Малахов А.С. Некоторые аспекты оперативно-розыскной характеристики мошенничеств, совершаемых дистанционным способом // Правопорядок: история, теория, практика. 2019. № 2. С. 77-81.