МИХАИЛ НИКИТИН,
преподаватель Учебного центра «Информзащита»

Введение

Если рассматривать деятельность террористических формирований и криминальных структур по подготовке и организации терактов и экономических преступлений, то условно их можно разделить на два больших кластера, включающих в себя: методы активных действий, с привлечением террористов-смертников и пассивные, дистанционные методы, с латентной формой протекания.

Организаторы терактов, как правило, используют современные телекоммуникационные технологии, находясь на значительном расстоянии от места совершения теракта. Эти методы позволяют им анонимно управлять активацией взрывных устройств и усложнять их поиск и обезвреживание.

А криминальные элементы, являясь иногда собственниками некоторых телекоммуникационных компаний, организуют различные серые схемы, связанные с незаконной терминацией межоператорского телефонного трафика. С одной стороны, это делается в целях снижения нагрузки на каналы, в целях экономии собственных средств, а с другой – подмена международного трафика и его пропуск под видом местного приносит колоссальную необлагаемую налогом прибыль, что в среде специалистов называется рефайлингом, на котором мы подробно остановимся в данной статье.

Актуальность предлагаемого материала связана со значительным распространением подобных преступлений не только в России, но и за рубежом, что в настоящее время привело к необходимости оперативного вмешательства уполномоченных федеральных, государственных и надзорных структур в процесс усовершенствования действующего законодательства. Данная мера необходима для выявления, предупреждения и пресечения преступлений в информационно-телекоммуникационной среде, и обеспечения эффективной защиты не только государственных и коммерческих структур, многочисленных социальных институтов, но и граждан Российской Федерации.

Проведенные исследования и системный анализ нормативно-правовой базы по данной категории преступлений, в сочетании с изучением самых распространенных методов телекоммуникационной преступности, позволяет говорить о наличии «слабых мест» в действующем российском законодательстве. В данной статье особое внимание будет сосредоточено на актуальных проблемах, возникающих на различных стадиях оперативного реагирования по делам телекоммуникационной направленности: на этапах выявления, расследования и их сопровождения, вплоть до стадии досудебного разбирательства.

SHUTTERSTOCK.COM/MIKKOLEM

Сформулированные тезисы, возможно, помогут законодателю внести существенные коррективы в нормативно-правовые акты и законодательную инфраструктуру РФ, в целях обеспечения правопорядка, охранительных мер виктимологического характера. Эти изменения позволят осуществить системные мероприятия по профилактике, предупреждению и пресечению преступных посягательств в информационно-телекоммуникационной среде и обеспечат возможность реализации превентивных мер, направленных на противодействие терроризму.

Термин «телекоммуникация» – достаточно емкое понятие, включающее в себя свыше 20 различных подкатегорий в алфавитном порядке, а с учетом международной интерпретации этого термина – 118. Но самое главное – все эти аппаратно-инструментальные технологии, как и все в нашем материальном мире, подвержены преступному посягательству. Даже сейчас, во времена современных развитых технологий, сведения о преступлениях в сфере телекоммуникации отрывочны. Пожалуй, сегодня никто в мире не имеет полной картины телекоммуникационной преступности. Государственные и коммерческие структуры, которые когда-либо подверглись кибератакам и прочим преступным посягательствам, не очень склонны афишировать данные об ущербе, причиненным этими атаками, поэтому случаи совершения телекоммуникационных преступлений становятся публично известными далеко не всегда.

ПО ДАННЫМ ИССЛЕДОВАНИЯ, КОТОРОЕ ЕЖЕГОДНО ПРОВОДИТСЯ БРИТАНСКОЙ АНАЛИТИЧЕСКОЙ КОМПАНИЕЙ ANALYSIS RESEARCH, ОБЩЕМИРОВОЙ УРОВЕНЬ ПОТЕРЬ «ТЕЛЕКОМОВ» ОТ КРИМИНАЛЬНЫХ АКТИВНОСТЕЙ В 2015 ГОДУ ДОСТИГ 43,5 % ОТ ВЫРУЧКИ, ПО СРАВНЕНИЮ С 25,1 %, В 2010-ОМ И 12,3 % В 2008-ОМ СООТВЕТСТВЕННО. В РОССИИ ПОТЕРИ ДОХОДЯТ ДО 84 % ОТ ПРИБЫЛИ

84%

Но даже те факты, которые становятся достоянием гласности, производят сильное впечатление.

Современный уровень развития информационно-телекоммуникационных технологий в России является очень высокодоходным бизнесом, а по своей технической и компьютерной оснащенности не уступает ни одной высокоразвитой сфере экономики. Поэтому неудивительно, что она как магнит притягивает к себе криминальный элемент всех мастей, причем уровень мошенничества в телекоммуникационном сегменте уже достиг масштабов организованного криминального бизнеса.

Преступники, которые ранее «специализировались» на продаже оружия, наркотиков, похищении людей, вооруженных ограблениях, кражах и т. д., постепенно «переквалифицировались» на освоение телекоммуникационного бизнеса. Ведь прибыли от преступной деятельности в этой сфере экономики не меньше, а риск значительно ниже, поскольку большая часть телекоммуникационных преступлений имеет скрытый характер протекания. В то же время российское законодательство пока не разработало каких-либо адекватных мер, направленных на борьбу с преступлениями такого рода.

По проработке вопросов защиты общества от такого рода преступлений западное законодательство, к сожалению, существенно опережает российское. Для примера, можно сравнить диспозиции некоторых статей УК РФ (действующая редакция) – ст. 159, 272, 273, 274 и раздел 18, параграфы 1029, 1030 и 1362 Примерного УК США 1962 г. за совершение различных мошеннических действий, где компьютер выступает лишь как орудие преступления. Так, в США для лиц, которые причиняют ущерб защищенным абонентским компьютерам, предусмотрены максимальные сроки наказания, которые колеблются от 10 до 25 лет лишения свободы. В России, за аналогичные преступления, предусмотрены меры: от условного наказания и до 7 лет лишения свободы. Нельзя не отметить такой факт, что в США компьютерные преступления причиняют ущерб, на порядок превышающий ущерб от других категорий преступлений. Интересна в этом плане статистика, опубликованная американскими экспертами. В США средняя оценка ущерба от одного физического ограбления банка составляет – 3,2 тыс. долл., от одного мошенничества – 23 тыс. долл., а от одной компьютерной кражи – 500 тыс. долл.

В России банки грабить как-то не принято, а жертвами ограблений, в основном, становятся инкассаторы. Однако, меру ответственности за грабеж по ч. 3 ст. 161 и за разбой ч. 4 ст. 162 УК РФ (до 15 лет) с американскими сравнивать сложно, т. к. Примерный УК США состоит из федеральных законов со своей точкой зрения на классификацию форм вины.

Уголовная ответственность за мошенничество в России (ст. 159 УК РФ), долгое время (с 1997 г. до 2013 г.) вообще не ужесточалась и мало чем отличалась по содержанию и срокам наказания от ст. 147 УК РСФСР. Такое «спящее» состояние российского уголовного законодательства сыграло на руку преступным элементам, которые, как известно, никогда не дремлют.

На заре развития телекоммуникационного бизнеса 90-х годов в России законодательные, судебные и исполнительные органы власти даже не могли спрогнозировать катастрофический рост преступности в этой отрасли экономики в последующие 10–15 лет. Некоторые брендовые «законодатели моды» современного телекоммуникационного бизнеса в свое время просто избежали уголовной ответственности за ранее совершенные ими преступления, ввиду отсутствия у вышеперечисленных структур элементарных знаний, опыта, методик расследования, приговоров по административным и уголовным делам, а, следовательно, и судебных прецедентов по данной категории преступлений. При этом первые успели «заработать» колоссальный капитал, выйти из тени, сформулировать и пролоббировать такие законы, которые сегодня им помогают уже

легально заниматься своим любимым делом, не подпуская новичков к источнику изобилия, поглощая более слабые компании.

К сожалению, именно такая тенденция наблюдается в развитии современного телекоммуникационного бизнеса не только в России, но и во всем мире, который по своей криминальной составляющей занял лидирующие позиции в списке таких тяжких преступлений, наряду с незаконным оборотом оружия и наркотиков. Так, по данным исследования, которое ежегодно проводится британской аналитической компанией Analysis Research, общемировой уровень потерь «телекомов» от криминальных активностей в 2015 году достиг 43,5 % от выручки, по сравнению с 25,1 %, в 2010-ом и 12,3 % в 2008-ом соответственно. В России потери доходят до 84 % от прибыли.

Для реализации своих преступных намерений в завладении денежными средствами государственных, коммерческих структур и просто российских граждан, мошенники применяют так называемые «серые схемы», например по «приземлению» междугородней и международной связи и сотового трафика, как правило, на свои же дешевые городские номера или на оборудование многочисленных дочерних операторов связи. Также известны многочисленные способы ситуационного психологического воздействия на граждан, связанных с вымогательством при совершении телефонного мошенничества (т. н. «развод» по телефону) и т. п.

Чем же вызвана подобная незащищенность российского потребителя телекоммуникационных услуг от преступных посягательств? В данном случае объектом посягательства являются правоотношения, возникающие между провайдерами, операторами связи, предоставляющие эти услуги и их потребителями, урегулированные соответствующими нормами права, но криминальные интересы третьих лиц (злоумышленников) вторгаются в эти правоотношения без ведома законных (легитимных) его участников, с целью извлечения собственной незаконной прибыли.

К настоящему времени существует достаточное количество примеров криминального воздействия (манипулирования) на некоторые виды телекоммуникационных услуг, которые при взаимодействии с финансовыми, правовыми, социальными институтами приобретают скрытое, негативное воздействие на них. При этом возникают некие, ранее неизученные элементы негласного, анонимного управления ими, которые в руках злоумышленников приобретают криминальный характер, становясь виртуальными орудиями преступления.

Но для того, чтобы предметно рассуждать о существующих проблемах телекоммуникационного бизнеса и получаемой аферистами колоссальной, необлагаемой налогом прибыли, необ-

ходимо, прежде всего, исследовать эти «серые» схемы незаконного обогащения. То есть, необходимо создать судебные прецеденты, которых нет по большей части из перечисленных преступлений телекомовской направленности. Для этого надо на стадии следствия собрать доказательную базу, затем, в рамках выдвинутой следствием версии обсудить выбранную диспозицию статьи Уголовного Закона с прокурором (потенциальным гособвинителем), чтобы он тоже понимал и разбирался, в предметной области, а также в материалах конкретного дела. Далее, собранные и проверенные соответствующими должностными лицами материалы уголовного дела направляются в суд. Но за обвинительный приговор еще придется побороться, т. к. у судов нет практики и, соответственно, нет ни обвинительных, ни оправдательных приговоров по уголовным делам данной направленности, что играет лишь наруку адвокатам и их доверителям в судебном процессе.

Учитывая слабую еще судебную практику по делам о телекоммуникационных преступлениях, можно только догадываться об уровне специальной подготовки большинства судей, которые, будучи профессиональными юристами, слабо разбираются в предметной области телекоммуникационных технологий.

Доказательства, связанные с этими преступлениями могут быть случайно изменены как в результате ошибок при их изъятии, так и в процессе самого исследования

Осложняет ситуацию и тот факт, что доказательства, связанные с этими преступлениями могут быть случайно изменены как в результате ошибок при их изъятии, так и в процессе самого исследования. Поэтому представление подобных доказательств в судебном процессе требует специальных знаний и соответствующей подготовки. Безусловно, как и обвинение, так и защита должны обладать этими специальными знаниями.

В связи с заявленным тезисом, мы считаем, что необходимо развивать институт независимых сертифицированных специалистов. Они бы могли давать квалифицированные заключения по техническим аспектам уголовных дел, проводить необходимые специальные (технические) исследования, давать экспертные заключения, имеющие доказательную правовую силу, а судейским корпусом воспринимались бы соответствующим образом – без сомнений. Эти же сертифицированные специалисты могли бы проводить специальные занятия, семинары по исследуемой тематике с судьями, прокурорами, следователями, участвовать в уголовных процессах как специалисты – консультанты, принимая на себя ответственность по ст. 307 УК РФ.

Необходимо понимать главное, то, что образует объективную и субъективную стороны состава таких преступлений. А именно, что все вышеперечисленные примеры не могут происходить без участия человека, следовательно, не могут быть немотивированными! Например, целью использования «серых» схем, в примере с пропуском и перенаправлением межоператорского междугороднего, международного и сотового трафика, является получение неучтенных доходов, а, следовательно, необлагаемой налогом колоссальной материальной выгоды, которая нигде и никем не декларируется, аккумулируясь в многочисленных оффшорах и «тихих местах».

Не менее значимым атрибутом «серых» схем, по степени опасности и тяжести последствий, является подмена номера. Все чаще «слепые» биллинговые сведения, получаемые оперативными подразделениями – субъектами ОРД, по постановлениям суда, не содержат точных сведений об абоненте, его месте нахождения, да и просто, номер телефона не соответствует действительности. Подобные случаи были впервые замечены силовиками при расследовании терактов на станциях метро Лубянка и Парк Культуры. В ходе анализа биллинга стационарных абонентских номеров, зарегистрированных в прилегающих к этим районам г. Москвы, было выявлено большое количество несоответствий.

Такое «загрязнение» биллинговой отчетности способствует увеличению числа латентных преступлений. Например, преступник, зная заранее о существовании такой «слепой» номерной емкости, находясь непосредственно в районе осуществления задуманных им преступных намерений, (из окна снимаемой им квартиры, автомобиля, либо просто используя мобильный сервис) сможет контролировать развитие той или иной криминальной ситуации которую он запланировал, например, дистанционно привести в действие взрывное устройство, осуществить поджог, остановить работу общественного транспорта, подвижных механизмов метро (эскалаторы), уничтожить средства

SHUTTERSTOCK.COM/REALINEMEDIA

коммуникации, инициировать сбой в работе телекоммуникационных сетей, сделать ложные вызовы скорой помощи, полиции, МЧС в совершенно противоположные районы от места ЧС и т. п. И что самое главное – преступника никто не найдет! Возникает логичный вопрос: кто несет ответственность за возникновение нелегального трафика, почему он вообще существует? Кто и как проверяет интерконнект-партнеров на прозрачность и честность? Очевидно, что данная проблема ещё не будировалась на правительственном уровне, а зря.

В этой связи подготовлен ряд тезисов-предложений для внесения дополнений в российское законодательство и усовершенствования ряда нормативно-правовых актов Российской Федерации.

Мы полагаем, что просто необходимо создать XIII Раздел в УК РФ, по аналогии с Налоговым Законом или IV Частью ГК РФ, где в настоящее время отражены все многочисленные нюансы незаконного использования объектов авторского права и смежных прав в совокупности с охраной товарного знака и знака обслуживания.

Этот Раздел мог бы называться: – «Преступления, совершаемые в информационно-телекоммуникационной сфере». Он мог бы начинаться, например, с главы 35 – преступления в информационной сфере; 36 – преступления в телекоммуникационной сфере; 37 – преступления в сфере связи и передачи данных, 38 – преступления, совершаемые с использованием мобильных (подвижных) средств связи, 39 – преступления, осуществляемые с использованием коротких номеров и мобильных приложений и т. д.

В этом Разделе должны быть собраны и квалифицированы все известные на текущий момент виды преступлений, совершаемые в информационно-телекоммуникационной среде. Эта инициатива исключит разное толкование правоприменителем тех статей УК РФ, которые в той или иной степени соответствуют телекоммуникационной направленности, но «разбросаны» по всей особенной части Уголовного Кодекса, начиная с ст.137–139.1 главы 19, раздела VII, ст.159–159.6, 165 главы 21, раздела VIII, ст.170–170.2, 180, 187 главы 22 и заканчивая ст. 272–274, главы 28 УК РФ раздела IX.

Предлагаемые нами меры сконцентрируют внимание законодательной, судебной и исполнительной властей на этом Разделе, будет накапливаться судебная практика по этой тематике, которая станет доступной для любого специалиста в виде разного рода бюллетеней суда, специализированных изданий, интернет источников с обзором уголовной практики по данной тематике.

Мы уверены, что просто необходимо в разы ужесточить меру уголовной ответственности за преступления, совершаемые в информационно-телекоммуникационной среде по аналогии с американским законодательством, где наглядность и широкая огласка выявленных и пресеченных преступлений носит хоть и жесткий, но не жестокий воспитательный характер.

Заключение

В своем коротком обзоре мы рассмотрели лишь некоторые примеры, законодательного, оперативного и просто гражданского реагирования в случаях, когда приходится лицом к лицу сталкиваться с преступными технологиями «развода на деньги». Мы привели примеры криминальных тенденций телекоммуникационного бизнеса, а также наиболее известные методы, которыми пользуются злоумышленники для достижения своих преступных намерений. Нами предложена их классификация и обозначена проблематика, связанная с выявлением, расследованием и оперативным сопровождением подобных преступлений. Но самое главное, мы хотели донести до понимания главный посыл, вытекающий из темы данного исследования: превентивные меры для обуздания преступности в информационно-телекоммуникационном сегменте российской экономики надо было предпринимать еще вчера. ●