DOI 10.22394/1818-4049-2017-81-4-182-187
УДК 343.721

А. С. Камко

Проблемы и перспективы системы противодействия мошенничеству с использованием телекоммуникационного и компьютерного оборудования

В статье рассматривается проблематика формирования и поддержания межведомственных структурных связей в сфере противодействия мошенничеству с использованием телекоммуникационного и компьютерного оборудования. Раскрывая основные проблемы формирования структурных связей между правоохранительными органами и представителями бизнес-сообщества, автор предлагает использовать для решения обозначенных проблем отечественный опыт взаимодействия органов исполнительной власти и коммерческих структур. Также автором определяются основные принципы, цели и задачи практического взаимодействия Министерства внутренних дел, предприятий финансового сектора и операторов связи. Кроме того, в статье учитывается существующая отечественная практика по вопросам информационного взаимодействия предприятий коммерческого сектора с правоохранительными органами и структурами государственной безопасности, позволяющая в некоторой степени игнорировать отказ операторов связи от взаимодействия с правоохранительными органами в рамках предлагаемой системы.

Ключевые слова: *мошенничество, противодействие мошенничеству, взаимодействие правоохранителей и бизнеса, обеспечение безопасности, предотвращение преступлений, социальная ответственность бизнеса.*

Одной из основных проблем практического противодействия мошенничеству, совершаемому с использованием телекоммуникационных и компьютерных сетей, является отсутствие устойчивых межведомственных структурных связей. В данном случае под межведомственными связями следует понимать такие методы и механизмы взаимодействия всех учреждений, при которых процессы нивелирования последствий совершенного противоправного деяния, блокирования путей совершения мошенничества, идентификации преступника и т. д. будут реализованы в кратчайшие сроки.

В начале 2013 г. расширенная рабочая группа экспертов, образованная при Министре внутренних дел (далее – МВД) Российской Федерации, подготовила предложения по дальнейшему реформированию органов внутренних дел (далее – ОВД) Российской Федерации. Данный документ был обозначен как «Дорожная карта». В п.п. 5, 6 данного документа было обозначено, что экспертам «представляется важным активизировать деятельность по противодействию киберпреступности. Следует разработать меры, в том числе законодательного плана, стимулирующие взаимодействие специализированных подразделений и операторов связи (сотовой связи, провайдеров и контент-провайдеров) в области обмена информацией и технологией; организовать целевую подготовку кадров в профильных гражданских вузах; шире использовать положения ФЗ «Об оперативно-розыскной деятельности» в части организации этого вида деятельности; обратить особое внимание на международное взаимодействие в данной сфере». [2]

Между тем в настоящее время вопросы взаимодействия правоохранительных

Камко Артем Сергеевич – доцент кафедры публичного и частного права, Дальневосточный институт управления – филиала РАНХиГС (г. Хабаровск). *E-mail: komandir.86@mail.ru*

органов и коммерческих структур, таких как банки, операторы связи (как мобильной, так и интернет-провайдеры) и прочие, остаются недостаточно проработанными с точки зрения рассматриваемой проблемы.

Следует отметить, что для различных организаций характерны разные подходы к вопросам управления рисками, связанными с мошенничеством, а также разная степень интенсивности соответствующих мер. Кроме того, мошенничество может принимать весьма разнообразные формы, а масштабы мошеннических действий, совершаемых сотрудниками и/или сторонними организациями и физическими лицами, значительно различаются в зависимости от того, о какой именно организации идет речь.

Так, например, рассматривая вопросы взаимодействия правоохранителей с банковским сектором, можно отметить следующее.

Современные банковские учреждения являются относительно закрытыми для контроля со стороны государства, в связи с чем в случае выявления признаков преступлений руководители банков обращаются за помощью в правоохранительные органы лишь в единичных случаях. Данное обстоятельство стало объективным условием выявления и документирования мошенничеств, совершаемых в сфере функционирования электронных расчетов, сотрудниками служб безопасности банков. Такое положение вещей вполне обосновано, поскольку нормативные документы большинства банковских учреждений РФ закрепляют такие обязанности служб банковской безопасности, как:

– выявление признаков подготавливаемых и совершенных преступлений, применение мер по их предупреждению и прекращению; подготовка материалов в правоохранительные органы для решения вопроса о возбуждении уголовного дела;

– участие в предварительном расследовании уголовных дел;

– направление правоохранительным органам информации, имеющей отношение к расследованию;

– применение в пределах компетенции мер по возмещению причиненного банку вреда.

Такие обязанности были закреплены в Приказе МВД России от 4 января 1996 г. № 4 «О реализации Соглашения между МВД России и Ассоциацией российских банков». Однако указанный Приказ утратил силу на основании Приказа МВД России от 26 февраля 2008 г. № 176 «О признании утратившим силу Приказа МВД России от 4 января 1996 г. № 4». Таким образом, отсутствие в законодательстве прямых предписаний по выполнению вышеперечисленных обязанностей приводит к тому, что на практике в большинстве случаев они не выполняются.

Данная ситуация является одной из основных причин столь высокого уровня латентности рассматриваемого вида деяний.

Как правило, в процессе «внутренних» проверок нарушения порядка осуществления банковских операций сотрудникам служб безопасности банков удается выявить приблизительно 10% – 15% мошенничеств, совершенных уполномоченными сотрудниками банков. Между тем, как справедливо указывает А. Ф. Волобуев, деятельность банков как структур рыночной экономики во многих аспектах связана с сохранением коммерческой (банковской) тайны. [2] Поэтому различного рода имущественные злоупотребления персонала банка становятся известными правоохранительным органам только тогда, когда на это даст разрешение руководство учреждения. Следует при этом отметить, что сотрудники банков, в частности сотрудники «младшего звена», занятые в работе с клиентами в операционных залах, регулярно фигурируют как лица, незаконно получающие и передающие (зачастую на возмездной основе) сведения, содержащиеся на банковских картах граждан.

Более тесное взаимодействие банков с органами предварительного расследования могло бы значительно ускорить процесс расследования преступлений данного вида, сделать его более эффективным. Результаты опроса, проведенного В. О. Финагеевым [3], показали, что совместная деятельность сотрудников банковской безопасности и следователей целесообразна в случаях:

– предоставления службами безопас-

ности правоохранительным органам материалов для решения вопроса о возбуждении уголовного дела (88% и 92%);

– доступа в помещения, к документам и техническим средствам банка, необходимым для проведения следственных действий, и оказания помощи в их применении (51% и 76%);

– налаживания связей и получения информации от иных банков по вопросам незаконного перечисления средств (42% и 68%);

– сбора и предоставления фактических данных, имеющих отношение к процессу расследования, с целью получения новых доказательств (74% и 92%);

– участия в розыске лиц, посягавших на интересы банка или подозреваемых в их совершении, а также применения в пределах компетенции мер по возмещению причиненного ущерба (35% и 44%).

Указанные данные свидетельствуют об осознании сотрудниками-практиками как со стороны правоохранительных органов, так и со стороны банковских учреждений необходимости решения отмеченных вопросов взаимодействия и закрепления их на законодательном уровне.

Ряд отечественных исследователей в целях решения возникающих проблем взаимодействия правоохранительных органов с банковскими учреждениями предлагают установить исчерпывающий перечень органов государственной власти, имеющих право получения из банков сведений, составляющих банковскую тайну, а также сроки предоставления информации, предусмотрев возможность их увеличения по просьбе банков. Кроме того, с целью сокращения временных рамок исполнения запросов правоохранительных органов, а также устранения необходимости нагромождения уголовного дела лишней информацией, рекомендуется предоставить банкам возможность передавать сведения, составляющие банковскую тайну, на электронных носителях с заверением ее подлинности в сопроводительных письмах.

Следует также отметить, что такие учреждения, как операторы связи (как мобильной, так и интернет-провайдеры), а также организации, деятельность которых связана с так называемыми виртуальными деньгами неохотно идут на контакт с правоохранительными органами.

Это порождает ситуацию, при которой само пострадавшее лицо вынуждено в ущерб прочим собственным интересам самостоятельно запрашивать и получать информацию от каждой из указанных структур. Однако в этом случае правоохранители получают объем данных, ограниченный полем деятельности либо контактов потерпевшего лица. Вопросы идентификации злоумышленника либо блокировки счетов в различных системах остаются отложенными на неопределенный срок. Во избежание затягивания проблемной ситуации нами уже была указана потребность адресного обращения в соответствующие инстанции со стороны граждан. Подобный подход, по нашему мнению, не является объективно исчерпывающим проблемную ситуацию и требует дальнейшей проработки.

Ряд исследователей в настоящее время сходится на идее о необходимости законодательного закрепления методов и механизмов взаимодействия правоохранительных органов с вышеобозначенными коммерческими структурами, четкой регламентации сроков предоставления данной информации и т. д.

По мнению автора, данный подход имеет рациональное основание, однако не учитывает различных аспектов социально-экономического взаимодействия субъектов российской экономики, ввиду которых столь радикальное влияние на права одних из крупнейших по своей структуре и финансовому обороту предприятий вызовет ряд значительных по своим масштабам негативных последствий.

При этом в отечественной практике существуют примеры разрешения подобных ситуаций, в которых требуется урегулировать вопросы общественных отношений в части интересов коммерческого сектора, государственных структур и неопределенного круга лиц аналогичными, но менее «жесткими» методами. Так, например, в марте 2015 г. ОАО «НК «Роснефть» и Федеральная антимонопольная служба России согласовали Стандарт, регламентирующий принципы ценообразования и порядок реализации Компанией

моторного топлива на внутреннем рынке РФ. Указанному Стандарту в настоящее время следуют все крупнейшие предприятия данного сектора экономики, а сам факт его принятия позволил урегулировать проблемы взаимодействия предприятий нефтеперерабатывающего комплекса и Федеральной антимонопольной службы РФ в вопросах, вызывающих некоторый общественный резонанс уже более десяти лет.

По аналогии с данным примером в настоящее время для разрешения вопросов взаимодействия правоохранительных органов и коммерческого сектора требуется разработка Регламента взаимодействия МВД, предприятий финансового сектора и операторов связи (далее – Регламент).

В рамках данного Регламента требуется определить:

– шаблон запроса на предоставление информации правоохранительным органам со стороны предприятий коммерческого сектора;

– сроки предоставления информации представителями коммерческого сектора по запросу из правоохранительных органов;

– формат предоставления данных (на бумажном или электронном носителе);

– способы заверения подлинности передаваемых данных;

– иные вопросы, относящиеся к полю деятельности правоохранительных органов.

Следует отметить, что обозначенный Регламент может являться частью некоторого Соглашения между всеми заинтересованными сторонами либо быть самостоятельным нормативным актом.

Предметом соглашения сторон в данном случае будет являться информационное взаимодействие и координация усилий по предотвращению случаев мошенничества с использованием телекоммуникационного и компьютерного оборудования (включая, но не ограничиваясь системами дистанционного банковского обслуживания), таких как оплата услуг путем отправки СМС-сообщений на «короткие номера»; оформление незаконных телефонных подписок; мошенничество с применением банковских карт и иных правонарушений в сфере обеспечения имущественных прав и законных интересов граждан.

Целями соглашения будут являться:

– предотвращение случаев мошенничества, минимизация ущерба и локализация последствий от неправомерных и недобросовестных действий сотрудников коммерческих учреждений и третьих лиц;

– предотвращение выплаты денежных средств, а также оплаты товаров и услуг посредством поддельных и фальсифицированных платежных карт;

– пресечение сделок с похищенным имуществом (банковскими картами, телекоммуникационным оборудованием) и имуществом, находящимся в розыске;

– выявление похищенного имущества граждан;

– профилактика мошенничества со стороны работников организаций-участников соглашения.

В рамках такого Соглашения коммерческие структуры будут обязаны:

– обеспечивать материально и организационно информационно-аналитическую работу по выявлению случаев и признаков мошенничества со стороны злоумышленников в пределах своей компетенции;

– обрабатывать запросы сотрудников и представителей ОВД в соответствии с технологией и регламентом информационного взаимодействия, определенными в ходе обсуждения и анализа технических возможностей, а также рациональных сроков исполнения обязательств сторон при согласовании проекта нормативного документа;

– использовать внешние источники информации и банки данных других ведомств в целях повышения эффективности информационного взаимодействия при условии соблюдения прав и законных интересов третьей стороны;

– оказывать содействие сотрудникам либо уполномоченным представителям ОВД в получении иной дополнительной информации о запрашиваемых объектах в интересах других организаций, подписавших аналогичное Соглашение, а также в интересах граждан (физических лиц), имущественные права которых были нарушены при совершении

преступления.

Органы внутренних дел также будут обязаны:

– оказывать содействие и методическую помощь организациям-участникам соглашения по вопросам выявления, профилактики и противодействия мошенничеству, совершаемому с использованием телекоммуникационного оборудования и компьютерных сетей;

– привлекать через заключение аналогичного Соглашения к участию в формировании системы профилактики и противодействия иные организации вне зависимости от формы собственности при условии, что деятельность (практически осуществляемая или информационного характера) данных организаций будет объективно полезна для функционирования указанной системы;

– обеспечивать непрерывность информационного взаимодействия и его инструктивно-методического сопровождения путем проведения информационно-практических мероприятий либо участия сотрудников правоохранительных органов в таковых по запросу от сторон-участников соглашения;

– периодически, при наличии возможности, направлять в адрес организаций-участников Соглашения в виде информационных записок и методических рекомендаций обобщенные материалы об имеющемся положительном опыте работы по профилактике правонарушений и проблемным вопросам защиты от мошенничества, а также событиях и фактах, требующих оперативного реагирования.

Следует также отметить, что при разработке и согласовании подобного Соглашения требуется учитывать существующую отечественную практику по вопросам информационного взаимодействия предприятий коммерческого сектора с правоохранительными органами и структурами государственной безопасности. Так, например, в соответствии с Постановлением Правительства РФ от 27 августа 2005 г. № 538 «Об утверждении Правил взаимодействия операторов связи с уполномоченными государственными органами, осуществляющими оперативно-розыскную деятельность» [1] одним из этапов определено предоставление оператором связи Управлению Федеральной службы безопасности (далее – УФСБ) по субъекту РФ – местонахождению сети связи баз данных (далее - БД) об абонентах, оказанных услугах связи (в т. ч. о соединениях, трафике и платежах абонентов). При этом информация предоставляется УФСБ путем осуществления круглосуточного удаленного доступа к БД и хранится в течение 3 лет. Исходя из этого, существует возможность игнорировать отказ от участия в предполагаемом Соглашении со стороны операторов связи при условии, что будет определен порядок предоставления доступа к имеющимся у них БД через технические возможности либо по запросу о предоставлении информации УФСБ по субъекту РФ – местонахождению сети связи.

Таким образом, будущее практического противодействия мошенничеству, совершаемому с применением телекоммуникационных и компьютерных сетей лежит в плоскости взаимодействия представителей коммерческого сектора и правоохранительных органов. При этом обеспечение безопасности коммерческих организаций представляется и элементом, и основой их деятельности. Состояние защищенности представляет собой умение и способность коммерческих организаций надежно противостоять любым попыткам криминальных структур нанести ущерб законным интересам предприятия и (или) физических лиц в рамках как поддержания имиджа коммерческой организации, так и «социальной ответственности» бизнес-структур.

Список литературы:

1. «Об утверждении Правил взаимодействия операторов связи с уполномоченными государственными органами, осуществляющими оперативно-розыскную деятельность» : Постановление Правительства РФ от 27.08.2005 г. № 538 // Собрании законодательства РФ. 2005. № 36. ст. 3704.

2. Анапольская А. И. Порядок взаимодействия правоохранительных органов с банковскими учреждениями при расследовании мошенничеств, совершаемых в сфере функционирования электронных расчетов // Вестник

ТГУ. 2015. № 5 (145). С. 221 – 224.

3. Финагеев В. А. Проблемы взаимодействия правоохранительных органов и подразделений банковской безопасности в выявлении и расследовании преступлений // Таможенное дело. 2013. № 2 (86). С. 264–270.

Библиографическое описание статьи

Камко А. С. Проблемы и перспективы системы противодействия мошенничеству с использованием телекоммуникационного и компьютерного оборудования // Власть и управление на Востоке России. 2017. № 4 (81). С. 182–187. DOI 10.22394/1818-4049-2017-81-4-182-187

A. S. Kamko

Problems and perspectives of the system for countering fraud using telecommunications and computer equipment

The article describes the problems of formation and maintenance of interdepartmental structural links in the sphere of counteracting fraud using telecommunication and computer equipment. Revealing the main problems of the formation of structural links between law enforcement agencies and representatives of the business community, the author suggests using the domestic experience of interaction between executive authorities and commercial structures to resolve the above problems. The author also determines the main principles, goals and tasks of practical cooperation between the Ministry of Internal Affairs, financial sector enterprises and telecom operators. In addition, the article takes into account the existing domestic practice on the issues of information interaction of enterprises of the commercial sector with law enforcement agencies and public security structures, which, to some extent, ignores the failure of communication operators to interact with law enforcement agencies within the framework of the proposed system.causes of victimization of certain groups of citizens are formulated. So, for a certain age category, this can be a banal ignorance about some aspects of cashless transactions, and for another - an excessively high level of trust, rendered to the strangers who called them. Based on statistical data and analytical conclusions, the subsequent development of the most effective victimization prevention methods for each of the selected groups is possible.

Keywords: *fraud, counter fraud, the interaction of law enforcement and business, security, crime prevention, social responsibility of business.*

References:

1. «Ob utverzhdenii Pravil vzaimodejstviya operatorov svyazi s upolnomochennymi gosudarstvennymi organami, osushchestvlyayushchimi operativno-rozysknuyu deyatel'nost'» : Postanovlenie Pravitel'stva RF ot 27.08.2005 g. № 538 // Sobranii zakonodatel'stva RF. 2005. № 36. st. 3704.

2. Anapol'skaya A. I. Poryadok vzaimodejstviya pravoohranitel'nyh organov s bankovskimi uchrezhdeniyami pri rassledovanii moshennichestv, sovershaemyh v sfere funkcionirovaniya ehlektronnyh raschetov // Vestnik TGU. 2015. № 5 (145). S. 221 – 224.

3. Finageev V. A. Problemy vzaimodejstviya pravoohranitel'nyh organov i podrazdelenij bankovskoj bezopasnosti v vyyavlenii i rassledovanii prestuplenij // Tamozhennoe delo. 2013. № 2 (86). S. 264–270.

Reference to the article

Kamko A. S. Problems and perspectives of the system for countering fraud using telecommunications and computer equipment// Power and Administration in the East of Russia. 2017. No. 4 (81). PP. 182–187. DOI: 10.22394/1818-4049-2017-81-4-182-187

Kamko Artem Sergeevich – Associate Professor of the chair of public and private law, the Far-Eastern institute of management – branch of RANEPA (Khabarovsk). *E-mail: komandir.86@mail.ru*