

УДК 343.1, 343.7, 343.72

DOI: 10.17223/23088451/17/12

О.В. Ханинева

**АКТУАЛЬНЫЕ ВОПРОСЫ ВЗАИМОДЕЙСТВИЯ СЛУЖБ И ПОДРАЗДЕЛЕНИЙ
ОРГАНОВ ВНУТРЕННИХ ДЕЛ ПРИ РАССЛЕДОВАНИИ УГОЛОВНЫХ ДЕЛ О МОШЕННИЧЕСТВАХ,
СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ
ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ**

Исследуются проблемные вопросы, возникающие при взаимодействии служб и подразделений органов внутренних дел, задействованных в раскрытии и расследовании уголовных дел о мошенничествах, совершенных с использованием информационно-телекоммуникационных технологий. Предложено несколько способов организации работы в данном направлении, позволяющих должным образом скоординировать ее, для принятия согласованных действенных решений и достижения целей уголовного судопроизводства.

Ключевые слова: *мошенничество, организация расследования, взаимодействие*

В различных сферах жизни идет активное внедрение современных цифровых технологий. Особенно это стало заметно в период пандемии.

Однако эти явления носят и отрицательный характер, например увеличение количества преступных посягательств, в основном на денежные средства граждан и организаций, с применением все тех же удобных, используемых в законных целях информационно-телекоммуникационных средств и технологий. Основную массу таких преступлений продолжают составлять мошенничества, способы совершения которых становятся все изощреннее, а их раскрытие – сложнее, ввиду их латентности и технической новизны используемых средств.

Ряд ученых в данной области, такие как А.Л. Осипенко, Н.Г. Муратова, М.С. Сергеев, неоднократно описывали наиболее часто встречающиеся способы совершения таких преступлений: рассылка SMS о победах в различных конкурсах; телефонные звонки из банков о блокировке карт; обращение родственников, попавших в дорожно-транспортные происшествия; переписка через взломанные страницы и аккаунты в различных социальных сетях с просьбой одолжить денежные средства; создание зеркальных интернет-сайтов либо интернет-магазинов; размещение объявлений на торговых площадках типа «Авито», «Юла» и т.п. [1. С. 109–110; 2].

Так, согласно отчетам о состоянии преступности в РФ, представленным порталом правовой статистики Генеральной прокуратуры РФ, за январь–февраль 2021 г. в стране выявлено свыше 309,3 тыс. преступлений. Это на 5,5% ниже, чем за аналогичный период прошлого года (далее – АППГ). В текущем году зарегистрировано почти 52 тыс. различных мошенничеств, что на 9,1% больше АППГ. Их доля в структуре преступности на протяжении последних лет последовательно увеличивалась и достигла 16,8%. Большинство мошенничеств (68%) совершено с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, их массив за последний год увеличился более чем на четверть (+26,7%, 35,5 тыс.). В Санкт-Петербурге (1,7 тыс.), Ленинградской (417), Тульской (351) областях их число возросло в два и более раза.

В целом на деяния в сфере информационно-телекоммуникационных технологий или компьютерной информации приходится одно из четырех регистрируемых преступлений (+29,4% 81,5 тыс.). Большинство киберпреступлений совершены с использованием сети Интернет (50,4 тыс.) или при помощи средств мобильной связи (32,8 тыс.) [3].

Полагаем, что вышеописанные показатели отражают реальную картину мошеннических атак на современное общество, которое не всегда успевает надлежащим образом их отражать.

Этому, по мнению автора, есть ряд объективных причин:

- использование мошенниками новейших возможностей информационно-телекоммуникационных технологий и сети Интернет;
- наличие знаний в технической области рассматриваемого вопроса (использование «подменных» телефонных номеров, создание «зеркальных» сайтов-двойников, использование программ-вирусов для внедрения в банковские системы и т.п.);
- достижение цели отсутствия личного контакта с потерпевшими;
- наличие способов дистанционного совершения и руководства сообщниками, а также распоряжения похищенным имуществом, вплоть до вывода денег на банковские счета, открытые вне пределов Российской Федерации, или на счета «неблагополучной» категории граждан;
- возможность перевода похищенных денег в криптовалюту и использование различных виртуальных кошельков, платежных систем вместо банковских счетов для совершения транзакций;
- низкая раскрываемость рассматриваемого вида преступлений, в том числе из-за отсутствия должной организации взаимодействия служб и подразделений ОВД РФ и оснащения техническими средствами и возможностями.

Несмотря на предпринимаемые ОВД РФ профилактические меры (демонстрация в средствах массовой информации видеороликов о способах совершения мошенничеств и борьбы с ними силами самих граждан; проведение бесед с социально незащищенными слоями

населения, такими как пожилые и одинокие люди; размещение листовок с предупредительными записями в общественных местах (остановки общественного транспорта, магазины, поликлиники и т.п.), они не являются достаточно действенными.

Становится очевидным, что в ходе выявления, раскрытия и расследования уголовных дел, связанных с совершением мошеннических действий, возникает ряд трудностей. Как отмечает С.Н. Казинская, «при совершении такого вида мошенничеств злоумышленники изначально выбирают способы хищения, при которых остается минимальное количество криминалистически значимой информации либо осуществляется сокрытие или уничтожение следов преступной деятельности, а также маскировка преступных действий под гражданско-правовые» [4. С. 68].

Своевременность и полнота расследования таких уголовных дел, несомненно, играют немаловажную роль в сборе доказательной базы, изобличению всех виновных в совершении преступления, установлении способов и средств хищения, блокирования банковских счетов, с помощью которых производятся незаконные транзакции с похищенными денежными средствами, блокирования незаконных интернет-сайтов и ресурсов с целью пресечения дальнейшего совершения преступлений, и несомненно, максимально полное возмещение причиненного потерпевшим вреда.

Помимо ряда принимаемых мер в этом направлении, по мнению автора, одной из существенных проблем, встающих на пути достижения обозначенных целей, остается необходимость пересмотра способов организации работы служб и подразделений ОВД РФ, задействованных в борьбе с мошенничествами.

Основными критериями для успешного раскрытия и пресечения мошенничеств, совершенных с использованием информационно-телекоммуникационных технологий и сети Интернет, являются следующие:

1) максимально короткий временной промежуток между совершением преступления и заявлением о данном факте в полицию;

2) установление принадлежности всех номеров телефонов, задействованных в совершении преступления, как со стороны потерпевшего, так и преступников;

3) быстрое получение детализаций телефонных переговоров и банковских выписок о движении денежных средств по счетам клиентов;

4) установление точного способа перевода похищаемых денежных средств (самостоятельное с собственной банковской карты через банкомат, онлайн-кабинет, терминал и т.п.);

5) установление наличия аудиозаписывающих программ в мобильном телефоне потерпевшего, позволяющих прослушать телефонные разговоры и в дальнейшем изъять образцы голоса преступника;

6) принятие мер к блокированию счетов, виртуальных кошельков, сайтов, объявлений и иных средств совершения преступления, с целью пресечения их дальнейшего совершения;

7) своевременное проведение оперативно-розыскных мероприятий и следственных действий;

8) проведение качественного анализа полученной информации по конкретному преступлению, а также совокупного анализа совершенных преступлений (по аналогии) на территории региона расследования на предмет совпадения способов совершения, используемых номеров телефонов, банковских карт и иных данных;

9) совместное обсуждение полученной информации, составление дополнительных планов взаимодействия, постановка задач исполнителям и сроков их исполнения;

10) разработка единого алгоритма выявления, раскрытия, расследования и пресечения мошенничеств рассматриваемого вида для использования всеми службами и подразделениями ОВД РФ;

11) налаживание электронного документооборота с операторами сотовой связи, интернет-провайдерами, банками, для сокращения сроков исполнения различных запросов и т.п.

Основываясь на собственном опыте работы в органах предварительного следствия и подразделениях уголовного розыска, а также мнению ряда ученых, в том числе Р.В. Кудрявцева, который в своей научной статье «Организация деятельности по раскрытию дистанционных мошенничеств» привел ряд примеров организации качественного взаимодействия [5. С. 218–221], предлагаем подробнее остановиться на такой форме взаимодействия, как проведение комиссионных заслушиваний расследуемых уголовных дел.

Попытаемся ответить на ряд вопросов: Что же предполагается при данной форме взаимодействия? Какова ее цель? Кто будет ее участниками? Каким документом оформляется начальный этап взаимодействия? Кто руководит процессом? Какова периодичность и порядок оформления решения таких совещаний?

Для начала следует дать определение понятию «взаимодействие». По мнению Д.Г. Шашина и П.В. Афанаскина, «взаимодействие» – это оказание следователями и сотрудниками оперативных подразделений взаимопомощи в решении общих, совместных задач уголовного судопроизводства [6. С. 33].

Автор согласен с таким определением, ввиду чего речь далее будет идти о возбужденных уголовных делах, по которым предварительное следствие обязательно с различным сроком следствия.

Что же такое «комиссионное рассмотрение уголовных дел» и какова их цель как формы взаимодействия? Предлагаем понимать это словосочетание как регулярное проведение неких совещаний руководством Следственного управления и Управления уголовного розыска субъекта РФ с участием и заслушиванием сведений из материалов уголовных дел, находящихся в производстве районных отделов полиции.

Правовой основой таких заслушиваний может послужить распоряжение или приказ начальника ГУ МВД России по субъекту или его заместителей, в ведении которых находится контроль за деятельностью следственных и оперативных подразделений.

В данном документе необходимо указать обоснование проведения комиссионных заслушиваний уголов-

ных дел о мошенничествах, определить и закрепить состав такой комиссии, назначить дату, место и время проведения совещания, определить проблемные вопросы и форму доклада.

К назначенной дате заслушивания ответственный сотрудник по линии работы как от следственного, так и от оперативного подразделения с участием своих руководителей должен провести детальный анализ находящихся в производстве уголовных дел и дел оперативного учета, подготовив при этом обзорные справки.

На самом комиссионном рассмотрении уголовных дел помимо сведений, указанных в обзорных справках, могут быть рассмотрены вопросы о новых способах взаимодействия с операторами сотовой связи, банками и т.п.; установление пробелов в организации работы в том числе по исполнению отдельных поручений следователя; ускорение получения ответов на запросы из организаций, обладающих интересующей следствие информацией; а также возможность привлечения их руководителей к административной ответственности ввиду неисполнения запросов правоохранительных органов; выработка новых решений и методов совместной работы.

Цель таких заслушиваний очевидна и состоит в обмене полученной информацией, а также выработке новых мер по выявлению, предупреждению, раскрытию и расследованию мошенничеств. Например, по ряду уголовных дел будет выяснен вопрос длительного исполнения (месяц и более) банками постановлений суда о выемке сведений, составляющих государственную и иную охраняемую законом тайну, в виде выписки движения денежных средств по счетам клиента с указанием дальнейших транзакций и личных сведений о других клиентах банка и т.п.

Действенной новой мерой, по результатам обсуждения, станет проработка вопроса о внедрении электронного документооборота с рядом российских банков, который позволит сократить сроки направления и получения соответствующих запросов и постановлений, касающихся предоставления информации, имеющей значение для уголовного дела.

Далее следует отметить, что на таких совещаниях происходит обмен информацией по всем уголовным делам, находящимся в производстве следователей под-

разделения на уровне района, и присутствие руководителей соответствующих управлений, при поочередном докладе, показывает общую картину проблем и недостатков на территории всего вверенного им субъекта. Это также позволяет выстраивать взаимодействие на должном уровне, уделяя особое внимание слабым местам, в том числе организовывая служебные командировки наиболее подготовленных сотрудников следствия и уголовного розыска для оказания практической помощи в отстающие подразделения.

На таких комиссионных рассмотрении уголовных дел выясняется специфика совершенных мошенничеств, например по способу хищения средств или общения с потерпевшим, использования одних и тех же номеров мобильных телефонов и т.п., что позволяет после доработки материалов ставить на рассмотрение вопрос о возможном соединении ряда уголовных дел (при наличии установленных законом оснований).

По итогам такого совещания возможно поставить задачи углубленного анализа уголовных дел при выраженном аналогичном способе совершения преступлений, для выявления фактов использования преступниками одной карты для хищения денежных средств, использования одного виртуального кошелька типа QIWI и т.п., использования одной SIM-карты или телефонного аппарата с одним IMEI.

Результаты комиссионного рассмотрения уголовных дел о мошенничествах предлагается оформлять соответствующим протоколом, в котором прописывать итоговые решения с назначением исполнителей, а также установлением сроков исполнения задач. Кроме того, назначается ответственное лицо, на которое возлагается контроль за исполнением принятых решений, из числа руководителей подразделений на уровне субъекта. Подписывают указанный протокол руководители заинтересованных подразделений, копия его направляется для исполнения на места.

Таким образом, по мнению автора, данный вид взаимодействия следственных и оперативных подразделений приведет к должной организации работы по противодействию мошенничествам, совершенным с использованием средств связи и сети Интернет, позволит повысить раскрываемость уголовных дел и увеличить количество задержанных лиц, их совершающих, в том числе на территории иных субъектов РФ.

ЛИТЕРАТУРА

1. *Осипенко А.Л.* Сетевая компьютерная преступность: теория и практика борьбы. Омск : Омская академия МВД России, 2009. С. 109–110.
2. *Муратова Н.Г., Сергеев М.С.* Правовое регулирование применения электронной информации и электронных носителей информации в уголовном судопроизводстве: отечественный и зарубежный опыт. М. : Юрлитинформ, 2019. 264 с.
3. *Портал* правовой статистики Генеральной прокуратуры РФ. URL: <http://crimestat.ru/analytics> (дата обращения: 19.04.2021).
4. *Казинская С.Н.* Актуальные проблемы расследования мошенничества // Таврический научный обозреватель. 2015. № 2. С. 119–125.
5. *Кудрявцев Р.В.* Организация деятельности по раскрытию дистанционных мошенничеств // Молодой ученый. 2019. № 24 (262). С. 218–221.
6. *Шагин Д.Г., Афанаскин П.В.* Сущность и назначение взаимодействия следственных и оперативных подразделений при расследовании преступлений // Научный компонент. 2019. № 2 (2). С. 33–41.

Статья принята к публикации 24.05.2021.

Topical Issues of Interaction Between Services and Departments of Internal Affairs Bodies in the Investigation of Fraud Committed Using Information and Telecommunication Technologies

Ugolovnaya yustitsiya – Russian Journal of Criminal Law, 2021, no. 17, pp. 58–61. DOI: 10.17223/23088451/17/12

Olga V. Khanineva, Krasnodar University of the Ministry of Internal Affairs of the Russian Federation (Krasnodar, Russian Federation).

E-mail: hanineva83@mail.ru

Keywords: fraud, organization of investigation, interaction

In the article, the author analyzes the growing problem of fraud committed using communications and the Internet in Russia and describes the interaction between the investigative and operational units of the Internal Affairs Departments of the Russian Federation aimed at detection, disclosure and investigation of this type of crimes. The author proposes certain quality improvements in the interaction between the units concerned to fight against crime, including electronic document flow with various organizations and institutions, as well as commission consideration of criminal cases in order to develop effective measures to combat fraud.

References

1. Osipenko, A.L. (2009) *Setevaya komp'yuternaya prestupnost': teoriya i praktika bor'by* [Network computer crime: combat theory and practice]. Omsk: Omsk Academy of the Ministry of Internal Affairs of Russia. pp. 109–110.
2. Muratova, N.G. & Sergeev, M.S. (2019) *Pravovoe regulirovanie primeneniya elektronnoy informatsii i elektronnykh nositeley informatsii v ugovnom sudoproizvodstve: otechestvennyy i zarubezhnyy opyt* [Legal regulation of the use of electronic information and electronic media in criminal proceedings: Russian and foreign experience]. Moscow: Yurlitinform.
3. The General Prosecutor's Office of the Russian Federation. (n.d.) *Portal of legal statistics of the General Prosecutor's Office of the Russian Federation*. [Online] Available from: <http://crimestat.ru/analytics> (Accessed: 19th April 2021).
4. Kazinskaya, S.N. (2015) Aktual'nye problemy rassledovaniya moshennichestva [Topical problems of fraud investigation]. *Tavricheskiy nauchnyy obozrevatel'*. 2. pp. 119–125.
5. Kudryavtsev, R.V. (2019) Organizatsiya deyatelnosti po raskrytiyu distantsionnykh moshennichestv [Organization of activities to uncover remote fraud]. *Molodoy uchenyy*. 24(262). pp. 218–221.
6. Shashin, D.G. & Afanaskin, P.V. (2019) Essence and importance of the collaboration between investigative and operational divisions in the investigation of crimes. *Nauchnyy component*. 2(2). pp. 33–41. (In Russian).

Received: 24 May 2021.