Полицейская деятельность
Правильная ссылка на статью:
Сидорова Е.З., Усов Е.Г., Алиев Т.Ф. К вопросу взаимодействия оперативных подразделений с банковскими учреждениями по преступлениям, совершаемым с использованием информационных технологий, в том числе сети Интернет // Полицейская деятельность. 2024. № 4. DOI: 10.7256/2454-0692.2024.4.70163 EDN: URPFQM URL: https://nbpublish.com/library_read_article.php?id=70163

К вопросу взаимодействия оперативных подразделений с банковскими учреждениями по преступлениям, совершаемым с использованием информационных технологий, в том числе сети Интернет

Сидорова Екатерина Закариевна

ORCID: 0000-0002-3477-3816

кандидат юридических наук

старший лейтенант полиции, заместитель начальника кафедры уголовного права и криминологии, Восточно-Сибирский институт МВД России

664017, Россия, Иркутская область, г. Иркутск, ул. Лермонтова, 110

eksid38@mail.ru

Усов Евгений Геннадьевич

ORCID: 0000-0002-5374-8346

кандидат юридических наук

доцент; Иркутский институт (филиал) Всероссийского государственного университета юстиции

664011, Россия, Иркутская область, г. Иркутск, ул. Некрасова, 4

eguirk38@mail.ru

Алиев Тимур Фирудинович

ORCID: 0000-0002-0645-931X

студент; институт 5 курс очной формы обучения ; Восточно-Сибирский институт МВД России

664017, Россия, Иркутская область, г. Иркутск, ул. Лермонтова, 110

timuraliev.2018@mail.ru

Статья из рубрики "Проблемы взаимодействия полиции с другими правоохранительными органами и институтами"

DOI:

10.7256/2454-0692.2024.4.70163

EDN:

URPFQM

Дата направления статьи в редакцию:

19-03-2024

Аннотация: Предметом настоящего исследования являются особенности взаимодействия оперативных подразделений органов внутренних дел с банковскими учреждениями по преступлениям, совершаемым с использованием информационно-телекоммуникационной сети Интернет. Цель работы заключается в рассмотрении и разрешении отдельных проблемных аспектов указанного взаимодействия. Актуальность выбранной тематики имеет как теоретический, так и практический аспекты значимости в современных реалиях. Так, в контексте динамичного роста преступлений с использованием информационных технологий, в том числе сети Интернет, является важным рассмотреть вопросы противодействия данному виду преступности. В современном мире названная категория преступности имеет злободневный характер в контексте её раскрытия и расследования. В 2023 г. Министерство внутренних дел Российской Федерации зарегистрировало 677 тыс. преступлений с использованием информационно-телекоммуникационных технологий, а в 2019 г. данный показатель составлял 294 тыс. 409 преступлений. Таким образом, речь идёт о двукратном увеличении совершения подобных преступлений за последние пять лет. Методология исследования основана на общенаучном и частнонаучных методах познания – диалектическом, логическом, статистическом, сравнительно-правовом, формально-юридическом, правового прогнозирования. Авторы представленной статьи пришли к выводу о том, что данная категория преступности выходит на первый план в силу динамичного роста совершения и вариаций её проявлений. В связи с этим важно рассмотреть вопрос об урегулировании на законодательном уровне сроков предоставления оперативно-значимой информации от банковских учреждений оперативным подразделениям в рамках производства оперативно-розыскных мероприятий по преступлениям, совершаемым с использованием информационно-телекоммуникационной сети Интернет. На первоначальном этапе сбор необходимых сведений зависит и от промежутка предоставления ответов банковских учреждений на запросы оперативных подразделений. В определенной степени это может повлиять как на своевременность, так и на эффективность раскрытия данных преступлений и причастных к ним лиц.

Ключевые слова:

интернет, преступность, мошенничество, вопросы взаимодействия, банковские учреждения, запросы, сроки предоставления, законодательное закрепление, эффективность, противодействие

В современных реалиях информационные технологии, в том числе информационно-телекоммуникационная сеть Интернет (далее по тексту — сеть Интернет), активно внедряются в жизнедеятельность человека и помогают ему реализовывать множество задач, например, электронное обучение, коммуникация в социальных сетях, запись к врачу через справочно-информационный интернет-портал «Госуслуги», покупки в интернет-магазинах, поиск необходимой информации в браузерах — всё это и многое другое становится возможным благодаря научно-техническому прогрессу.

В настоящем исследовании автором изучены труды, в том числе монографии отечественных ученых Р. И. Дремлюга [1], А. П. Агаповой [2], В. В. Буряка [3], С.П. Бутко [4], О. А. Самсоновой [5] и др., многие из которых являются признанными учеными в области противодействия преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий (далее — ИТТ). Методология настоящего исследования основана на общенаучном и частнонаучных методах познания — диалектическом, логическом, статистическом, сравнительно-правовом, формально-юридическом, правового прогнозирования. Авторы статьи, суммировав различные точки зрения по заявленной теме, в дальнейшем приводят собственную позицию по исследуемой проблематике.

Развитие информационных технологий, в частности, сказалось и на новых способах совершения киберпреступлений [6, с. 101]. К сожалению, следует констатировать тот факт, что цифровые технологии, значительно улучшая жизнедеятельность современного человека, точно так же несут в себе и потенциальную опасность для него, поскольку количество и вариативность преступлений в сфере информационных технологий (далее – IT-преступлений) возрастают практически ежегодно. Как верно отметили В. Б. Вехов и П. С. Пастухов, «использование преступниками ИТТ в качестве средств совершения преступлений приобретает повсеместный характер, ведет к появлению новых способов совершения преступлений» [7, с. 131].

Считаем заслуживающей внимания позицию Президента Российской Федерации, который на ежегодном расширенном заседании коллегии Министерства внутренних дел Российской Федерации (далее — МВД России) подчеркнул, что «один из безусловных приоритетов вашей работы — это борьба с преступностью с использованием информационных технологий. По итогам 2022 года число таких преступлений превысило полмиллиона и составило четверть от всех уголовно наказуемых правонарушений». Действительно, противодействие преступлениям с использованием ИТТ становится для правоохранительных органов едва ли не первоочередной задачей в их повседневной деятельности.

Исследование криминогенной обстановки в Российской Федерации показывает, что количество преступлений, связанных с ИТТ, имеет тенденцию к росту [8, с. 193], и это подтверждается следующими статистическими данными:

1. В 2023 г. МВД России было зарегистрировало 677 тыс. IT-преступлений в стране, что стало рекордным уровнем за всё время, как отмечает газета «Известия» со ссылкой на базу ведомства.

2. В 2022 г. было выявлено более 522 тыс. преступлений, совершаемых с использованием ИТТ, что составляло 22 % от общего количества противоправных деяний.

3. В предыдущие годы ситуация выглядела таким образом: в 2021 г. было зарегистрировано 706 тыс. 7 преступлений с использованием ИТТ или в сфере компьютерной информации, в 2020 г. — 510 тыс. 4 преступления; в 2019 г. — 294 тыс. 409 преступлений

По мнению Н. В. Вирясовой и А. Н. Земляновой, причинами такого аномального роста преступлений в данной сфере является стремительное понижение доходов и, соответственно, низкий уровень жизни граждан; снижение престижа труда; отсутствие у большей части населения знаний о соблюдении мер безопасности при работе и

приобретении товаров в сети Интернет; технические ошибки и несовершенства систем интернет-банкинга; низкий уровень подготовки сотрудников правоохранительных органов в сфере раскрытия и расследования дистанционных преступлений; отсутствие должного взаимодействия сотрудников органов внутренних дел (далее — ОВД) с интернет-провайдерами, операторами мобильных сетей и службами безопасности банков [9, с. 49].

На сегодняшний день становится всё более злободневным вопрос о хищении денежных средств со счёта владельца банковской карты путем совершения в отношении него мошеннических действий. Несомненно, безналичный вид расчётов становится всё более востребованным для общества, но в то же время необходимо сказать и о различных способах завладения безналичными денежными средствами. Данные способы непрерывно совершенствуются, развиваются и обновляются, появляются и совершенно новые [10]. Так, метод кражи безналичных денег при помощи скримминга с карты заключается в копировании данных магнитной ленты банковской карты, а затем в создании её копии с целью дальнейшего получения денежных средств (снятие их с копии банковской карты). Другой метод – фишинговые атаки, сущность которых заключается в подмене официального сайта банка на сайт её точной копией, при этом заметить разницу можно только по маленькой опечатке в адресе сайта. Ещё один способ – бесконтактные ридеры, которые используются для считывания данных банковских карт на незначительном расстоянии. Достаточно лишь на 5-10 см приблизить такой ридер к карте, и нужная информация перейдёт к злоумышленникам, которые смогут изготовить её копию и будут списывать небольшие суммы с высокой скоростью [11, с. 190].

С уголовно-правовой точки зрения необходимо сказать, что преступления с использованием ИТТ, в том числе сети Интернет, могут квалифицироваться по различным статьям Уголовного кодекса Российской Федерации (далее — УК РФ), например:

1. организация деятельности, направленной на побуждение к совершению самоубийства, сопряжённая с использованием информационно-телекоммуникационных сетей (включая сеть интернет) (ч. 2 ст. 110.2 УК РФ);

2. склонение к совершению самоубийства или содействие совершению самоубийства, совершенные в информационно-телекоммуникационных сетях (включать сеть интернет) (пункт «д» ч. 3 ст. 1101 УК РФ);

3. клевета, совершённая публично с использованием информационно-телекоммуникационных сетей (включая сеть интернет) (ч. 2 ст. 128.1 УК РФ);

4. насильственные действия сексуального характера, совершённые с использованием сети интернет, в отношении лица, не достигшего четырнадцатилетнего возраста (п. «б» ч. 4 ст. 132 УК РФ);

5. развратные действия, совершенные с использованием информационно-телекоммуникационных сетей (включать сеть интернет) (ст. 135 УК РФ);

6. нарушение авторских и смежных прав, сопряжённое с неправомерным доступом к компьютерной информации и (или) созданием, использованием вредоносных компьютерных программ (ст. 146 УК РФ по совокупности со ст. 272 УК РФ и (или) ст. 273 УК РФ);

7. мошенничество с использованием электронных средств платежа, сопряжённое с неправомерным доступом к компьютерной информации и (или) созданием,

использованием и распространением вредоносных компьютерных программ (ст. 159.1 УК РФ по совокупности со ст. 272 УК РФ и (или) ст. 273 УК РФ);

8. кража, сопряжённая с неправомерным доступом к компьютерной информации и (или) созданием, использованием вредоносных компьютерных программ (ст. 159.1 УК РФ по совокупности со ст. 272 УК РФ и (или) ст. 273 УК РФ);

9. мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ);

10. изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних, совершенные с использованием информационно-телекоммуникационных сетей (включая сеть интернет) (п. «г» ч. 2 ст. 2421 УК РФ) и др.

Стоит сказать, что мошенничества с использованием ИТТ, в том числе сети Интернет, имеют следующие вариации проявлений:

1) мошенничество, совершённое через сайты объявлений (схема «мошенник — продавец»);

2) мошенничество, также совершённое через сайты объявлений (схема «мошенник — покупатель»);

3) мошенничество со взломом страниц социальных сетей;

4) мошенничество с использованием интернет-сайтов;

5) мошенничество, совершённое под предлогом заказа банкета;

6) мошенничество, совершённое под предлогом совершения операций по банковским картам;

7) мошенничество, совершённое под предлогом помощи родственнику, попавшему в беду;

8) мошенничество, совершённое под предлогом компенсации за ранее приобретенные биологически активные добавки;

9) мошенничество, совершённое с использованием вредоносных программ на операционной системе Android;

10) мошенничество, совершённое с использованием социальных сетей (интернет-магазин в социальной сети «ВКонтакте») и др.

В этой связи стоит акцентировать внимание на точке зрения С. А. Нольдта, отметившего, что своевременное проведение полноценного комплекса оперативно-розыскных мероприятий (далее — ОРМ) на первоначальном этапе расследования позволяет в короткий срок задокументировать механизм преступной деятельности, установить причастных к его совершению лиц и получить достоверные доказательства. При этом важно выделить перечень действий оперативного сотрудника по первоначальным и последующим действиям в рамках выявления и раскрытия преступления [12, с. 70].

В первую очередь оперативному сотруднику необходимо получить объяснение с лица, в отношении которого совершено или совершается данная категория преступности, и выяснить следующие сведения оперативно-значимого характера: номер телефона злоумышленника; сведения об интернет-источнике (например, если речь идёт об объявлении на «Авито», «ВКонтакте» и др.); адрес электронный почты преступника

(например, если переписка осуществлялась таким образом или он предоставлял о ней сведения); сведения о злоумышленнике (как он представлялся заявителю); содержание SMS-сообщений (если таковые сведения имеются) и др.

Продолжая развивать мысль о деятельности оперуполномоченных при раскрытии исследуемой нами категории преступности, необходимо отметить и перечень проводимых оперативно-технических мероприятий. С учётом того, что интернет обеспечивает возможность передачи данных по различным каналам связи, то оперуполномоченный проводит следующие ОРМ:

- ОРМ «Снятие информации с технических каналов связи» — проводится на основании судебного разрешения и сущность его заключается в возможности получении, преобразовании и фиксации всех возможных видов связей (кроме телефонной связи), их сканировании и в последующем установления местоположения объектов мероприятия (злоумышленников) и определения их абонентских номеров;

- ОРМ «Прослушивание телефонных переговоров» — сущность данного мероприятия заключается в прослушивании акустической информации, передаваемой по каналам телефонной связи. Данное мероприятие может использоваться при прослушивании телефонных звонков (в том числе мессенджерах WhatsApp, Viber и др), телексных и факсимильных сообщений, передаваемой фотоматериалам, видеоинформации и тд;

- ОРМ «Получение компьютерной информации» — сущность данного мероприятия заключается в копировании и изъятии сведений, хранящиеся в специализированной информационной системе или в получении информации, содержащейся на компьютерных носителях, в которые заблаговременно были внедрены закладные компьютерные устройства и (или) программные компоненты и др.

Также необходимо отметить ОРМ «Обследование зданий, сооружений, участков местности, транспортных средств и земельных участков» — сущность которого заключается в гласном или негласном проникновении в жилые или нежилые помещения с целью обнаружения, физического изъятия предметов, которые могут иметь причастность к совершению преступлений. Например, если есть сведения о том, что у мошенника содержится по месту проживания компьютер, с которого осуществлялись мошеннические действия, оперуполномоченный производит их изъятие в порядке ОРМ «Сбор образцов для сравнительного исследования» для их дальнейшего изучения в ходе ОРМ «Исследование предметов и документов».

По мнению Ю. В. Бирюковой, если речь идёт о краже, совершённой с использованием средств сотовой связи (когда лицо добровольно предоставило злоумышленнику сведения о своих счетах, номере карты, паролях из SMS-сообщений и др.), то оперативному сотруднику следует провести ОРМ «Опрос» и уточнить следующую оперативно-значимую информацию [13, с. 140]:

1) детализацию телефонных соединений за период общения потерпевшего с подозреваемым;

2) расширенную выписку о движении денежных средств по счету потерпевшего, а также сведения о наличии либо отсутствии подключённой услуги «мобильный банк» с указанием абонентских номеров; все чеки, квитанции, интернет-переписку, выписки по банковскому счету, банковскую карту, со счета которой похищались денежные средства, снимок экрана (скриншот) переписки с мошенником, сохранившейся у потерпевшего;

3) уточнить у потерпевшего, в какой именно банк были перечислены денежные средства.

С учётом данной информации выглядит целесообразным получить в ходе проведения ОРМ «Наведение справок» от банковских учреждений сведения о мошеннических действиях следующего характера:

во-первых, сведения о владельце банковской карты: фамилию, имя, отчество (далее — Ф. И. О.), дату рождения, адрес проживания (прописки), место работы (учёбы), по возможности фотографию с изображением лица, на чье имя потерпевшим отправлен перевод. Данные сведения необходимы для установления личности и дальнейшей «отработки» причастности подозреваемого лица к совершению преступления.

во-вторых, информацию о месте и времени транзакций в момент перевода денежных средств заявителем (потерпевшим), с целью изучения возможных маршрутов и мест использования перечисленных на счёт потенциального мошенника денежных средств;

в-третьих, данные о предыдущих операциях по счету с целью определения образцов поведения и возможных предварительных действий потенциального мошенника;

в-четвертых, информацию о регулярно оплачиваемых абонентских номерах (личный номер, номер родственников или друзей);

в-пятых, информацию об абонентских номерах, привязанных к данной банковской карте услугой «мобильного банка», где и каким образом они были подключены;

в-шестых, информацию об адресе офиса банка, в котором была открыта банковская карта;

в-седьмых, иные сведения, которые помогут раскрытию преступления: IP-адреса; мобильные устройства, используемые для операций; адреса электронной почты и др.

Например, при получении информации о транзакциях либо о предыдущих операциях по счетам потенциального мошенника возможно провести различные ОРМ в зависимости от конкретной ситуации:

1) путем проведения личного сыска (комплекса ОРМ, проводимых лично оперуполномоченным) «отработать» места, где производились банковские операции (предположим, продуктовые магазины). В данной ситуации оперативный сотрудник посещает подобные локации, просматривает при соответствующем запросе видеокамеры на установление изображения злоумышленника, далее проводит ОРМ «Опрос» в отношении сотрудников магазинов, их владельцев, посетителей на предмет того, видели ли они данное лицо, как часто они видят его, какие особые приметы они могут выделить, родственные и иные связи, возможные пути следования, какие дополнительные данные об изучаемом лице могут предоставить и т. д.;

2) с наличием конкретной информации оперативный сотрудник путем проведения ОРМ «Наблюдение» проверяет возможные маршруты потенциального мошенника: в каком направлении он направился (при просмотре записи видеокамер), какие продуктовые магазины имеются рядом; также путем ОРМ «Опрос» стоит установить контакт с местными жильцами, с так называемыми старшими по дому, чтобы уточнить оперативно-значимую информацию о данном лице, проживало или проживает и как давно, как часто появляется, с кем живёт, контактные данные лица и т. д.;

3) при наличии информации о Ф. И. О. возможно провести легендированный опрос в

отношении конкретных лиц. Например, если на месте ранее совершённых банковских операций нет чёткого изображения на записи видеокамеры лица, возможно разведать информацию путем проведения ОРМ «Опрос», при этом не выдавая цель проводимого оперативным сотрудником мероприятия. Объектами данного опроса могут быть: родственники потенциального мошенника, друзья, бывшие осуждённые и др. ОРМ проводится с мотивом негласного сбора оперативно-значимой информации без разглашения его конкретной цели;

4) при наличии сведений об образе жизни лица, например, если оно (лицо) зависимо от алкогольной продукции и систематически её употребляет, стоит узнать «местные точки» сбора лиц, периодически собирающихся в данных местах для распития алкоголя; «отработать» в ближайшей расположенности магазины с алкогольной продукцией (например, «Бристоль», «Виноград», магазин разливного пива) и др.

Стоит сказать, что данные сведения возможно «отработать» только при первоначальном установлении сведений о потенциальном мошеннике, где немаловажная роль отводится банковским учреждения, потому что от своевременности предоставляемых ими ответов на запросы оперативных сотрудников в определенной степени зависит процесс раскрытия преступлений и установления причастных к ним лиц.

Также согласимся с мнением Е. И. Третьяковой и А. И. Белькова о том, что одним из важнейших вопросов в рамках оптимизации расследования дистанционных мошенничеств является определение сроков предоставления банковских данных [14, с. 141].

В этой связи, с учётом позиций Д. Г. Шашина, стоит более детально стоит остановиться на получении сведений оперативно-значимого характера от банковских учреждений. Сотрудник оперативного подразделения при проведении проверки полученной информации направляет соответствующие запросы в банки и другие кредитные организации в рамках проведения ОРМ «Наведение справок», но указанные учреждения зачастую отказываются отвечать на них, ссылаясь на ст. 26 Федерального закона от 2 декабря 1990 г. № 395-1 «О банках и банковской деятельности» (далее — закон о банках и банковской деятельности) [15, с. 79].

Отметим, что в соответствии с п. 6 ст. 11 Федерального закона «О службе в органах внутренних дел Российской Федерации и внесении изменений в отдельные законодательные акты Российской Федерации» от 30 ноября 2011 г. № 342-ФЗ (ред. от 04.08.2023, с изм. от 26.02.2024), сотрудник полиции (оперативного подразделения ОВД) имеет право на доступ в установленном порядке к сведениям, составляющим государственную тайну, если выполнение служебных обязанностей по замещаемой должности связано с использованием таких сведений.

Принимая во внимание тот факт, что действия сотрудников оперативных подразделений полиции по направлению запросов в кредитные организации обусловлены выполнением возложенных на них обязанностей по выявлению, предупреждению, пресечению и раскрытию преступлений, а также тот факт, что указанные действия соответствуют правам сотрудников ОВД, предоставление информации, отнесенной к профессиональной тайне, по запросам полиции не может быть расценено как ее разглашение.

Существующий порядок предоставления сведений, содержащих банковскую тайну, не имеет чёткой правовой регламентации, в результате чего и возникают проблемы при взаимодействии с кредитными организациями. Согласно действующему

законодательству, банки вправе не предоставлять какую-либо информацию относительно счетов юридических и физических лиц, движении их денежных средств, о структурировании безналичных денежных средств с использованием банковских счетов, поскольку данная информация охраняется правом на банковскую тайну.

Стоит отметить, что вопрос о предоставлении банковских сведений оперативным подразделениям решается на законодательном уровне. Так, согласно Федеральному закону «О внесении изменений в статью 26 Федерального закона "О банках и банковской деятельности" и статью 27 Федерального закона "О национальной платежной системе"» от 20 октября 2022 г. № 408-ФЗ, Центральный банк Российской Федерации (далее — Банк России) и сотрудники полиции обязаны осуществлять обмен данных о мошеннических действиях с соблюдением норм банковской тайны. Для Банка России это является возможностью предотвращать новые мошеннические операции.

Так, на основании полученных от МВД России сведений о совершенных противоправных действиях Банк России будет предоставлять полиции информацию о случаях и попытках переводов денежных средств, осуществленных без согласия клиента. С этой целью МВД России добавлено в состав пользователей Автоматизированной системы обработки инцидентов ФинЦЕРТ Банка России (АСОИ ФинЦЕРТ). Также между МВД России и Банко России заключено соглашение, регулирующее порядок информационного обмена, форму и перечень предоставляемых сведений. Изменения в законодательство Российской Федерации вызваны большим количеством дистанционных хищений денежных средств, в том числе с использованием методов социальной инженерии. Несомненно, оперативное взаимодействие МВД России с Банком России позволит эффективно решать вопросы профилактики, пресечения и раскрытия данных преступлений.

Однако при этом вышеназванным законом не был урегулирован срок предоставления указанных сведений оперативным подразделениям.

Приведенный анализ показывает, что основная результативность в получении информации оперативно-значимого характера зависит от взаимодействия ОВД с банковской сферой [16, с. 152].

В этой связи также важно сказать, что «виртуальные» преступники чаще всего совершают противоправные деяния не в местах своего постоянного пребывания, и зачастую установление их местонахождения и привлечение к установленной законом ответственности становятся менее вероятными. Проблема раскрываемости этих преступлений заключается в том, что их большая часть совершается в виртуальной среде, что не позволяет своевременно выявить лиц, причастных к свершению таких преступлений.

Согласимся с точкой зрения Ю. В. Гаврилина, ссылающегося на практику, о том, что оперативное сопровождение расследования уголовных дел осуществляется лишь на первоначальном этапе, «по горячим следам», до установления лица, подлежащего привлечению в качестве обвиняемого. В дальнейшем эффективность оперативного сопровождения в рамках установления обстоятельств, имеющих значение для доказывания по уголовному делу, снижается [17, с. 147—148].

В соответствии с порядком рассмотрения сообщений о преступлении, указанным в ст. 144 Уголовно-процессуального кодекса Российской Федерации, уполномоченные на то лица должны принять по нему решение не позднее трёх суток, с возможностью продления при наличии законных на то оснований до десяти и тридцати суток

соответственно с разрешения продления должностных лиц, указанных в третьей части настоящей нормы. Тем не менее стоит акцентировать внимание исследователя на том, что банковские учреждения периодически ссылаются на деловую загруженность и откладывают ответы по предоставлению необходимых сведений оперативно-значимого характера оперативным сотрудникам.

Бесспорно, банковские учреждения выполняют важные задачи по кредитованию и прочему обслуживанию физических и юридических лиц, проведению денежных расчетов и кассового обслуживания клиентов, выпуску, покупке, продаже платежных документов и ценных бумаг (учет векселей и операций с ними; операций с ценными бумагами; управлению имуществом клиентов по доверенности) и т. д. И всё же стоит акцентировать внимание на предоставлении ответов на запросы оперативных подразделений, в первую очередь для более своевременного противодействия рассматриваемой категории преступлений.

Таким образом, информационные технологии, в том числе сеть Интернет, кроме своих явных преимуществ для человека в контексте их применения с целью осуществления им повседневных, профессиональных и иных задач, используются злоумышленниками для реализации противоправных деяний. Исследуя криминогенную обстановку, мы пришли к выводу, что количество совершенных IT-преступлений имеет тенденцию к росту. Так, например, их количество с 2019 г. (294 тыс. 409 преступлений) по 2023 г. (677 тыс. преступлений) выросло более чем в 2 раза.

С учётом приведённых первоначальных и последующих ОРМ, проводимых сотрудниками оперативных подразделений территориальных органов МВД России, в первую очередь оперативному сотруднику необходимо получить объяснение с лица, в отношении которого совершено или совершается данная категория преступности. На данном этапе является важным сбор оперативно-значимой информации для проведения дальнейших мероприятий (в том числе оперативно-технических мероприятий, например, таких как «Прослушивание телефонных переговоров», «Снятие информации с технических каналов связи», «Получение компьютерной информации»). Так, оперативный сотрудник уточняет следующую оперативно-значимую информацию: способ совершения преступления (через «Авито», «Вконтакте», «WhatsApp» и тп.); на какой банковский счёт были денежные средства; номер телефона злоумышленника и сведения о нём (как он представлялся заявителю); содержание SMS-сообщений (если таковые сведения имеются) и др.

В последующем проводятся мероприятия по идентификации потенциального преступника, установлению его местонахождения, проведению в отношении него дальнейших ОРМ и следственных действий, а также для привлечения к установленной законом ответственности (при наличии законных оснований). При этом, оперативное сопровождение расследования уголовных дел осуществляется лишь на первоначальном этапе, «по горячим следам», в дальнейшем эффективность для установления всех обстоятельств, имеющих значение для доказывания по уголовному делу, снижается.

Несомненно, данная категория преступности требует от сотрудников полиции выработки мер по интенсификации её противодействия. Отметим, что виртуальные злоумышленники регулярно разрабатывают новые схемы совершения своих преступных деяний и постоянно меняют места своей дислокации, что в целом осложняет осуществление раскрытия исследуемой категории преступности. В этой связи, с учётом мобильности IT-преступников, является важным в максимально возможный короткий срок осуществлять мероприятия по установлению их местонахождения. Как было отмечено ранее, эффективность раскрытия данной категории преступности зависит от взаимодействия

оперативных подразделений с банковскими учреждениями, в том числе сроков предоставления от последних ответов на запросы в рамках проведения ОРМ «Наведение справок».

Видится, что в целях своевременного и более эффективного раскрытия, расследования и предотвращения преступлений в сфере ИТТ, в том числе сети Интернет, а также установления причастных к ним лиц, является важным проработать на законодательном уровне вопрос о конкретизации сроков предоставления информации оперативным сотрудникам от банковских учреждений.

С учётом вышеизложенного и принимая во внимание отсутствие законодательного закрепления сроков предоставления оперативно-значимой информации от банковских учреждений, авторы статьи полагают целесообразным дополнить статью 8 Федерального закона «Об оперативно-розыскной деятельности» от 12 августа 1995 г. № 144-ФЗ следующим содержанием:

«В рамках проведения оперативно-розыскного мероприятия „Наведение справок" по преступлениям, совершаемым с использованием информационных технологий, в том числе сети Интернет, оперативные подразделения по направляемым запросам в банковские учреждения делают отметку о необходимости предоставления обратного ответа в течение 72 часов с целью своевременного выявления и раскрытия данной категории преступлений и установления причастных к ним лиц, в том числе их местонахождения».

Несомненно, оперативным подразделениям как носителям профессиональной информации, т. е. не подлежащей разглашению, и, помимо этого, с целью более эффективного и своевременного выявления и раскрытия преступлений, совершаемых с использованием сети Интернет, видится важным закрепление на законодательном уровне сроков предоставления сведений оперативным сотрудникам от банковских учреждений.

Библиография

1. Дремлюга Р. И. Уголовно-правовая охрана цифровой экономики и информационного общества от киберпреступных посягательств: доктрина, закон, правоприменение, 2022. – С. 328.
2. Агапов П. В. Противодействие киберпреступности в аспекте обеспечения национальной безопасности. Агапов П. В., Борисов С. В., Вагурин Д.В., Коренюк А.Л., Меркурьев В.В., Побегайло А.Э., Халиуллин А. И. Москва: Юнити, 2014. – С. 512.
3. Буряк В. В. Цифровая экономика, хактивизм и кибербезопасность: Монография. – Симферополь: ИП Зуева Т.В., 2019. – С. 140.
4. Бутко С. П. Взаимодействие правоохранительных органов с банковскими учреждениями // Экономические исследования и разработки, 2022. – С. 38-43.
5. Самсонова О. А. Получение органами предварительного расследования и судом информации, составляющей банковскую тайну: автореф. дисс. канд. юрид. наук: спец. 12.00. 09 В«Уголовный процесс, криминалистика и судебная экспертиза, оперативно-розыскная деятельностьВ» // Иркутск, 2003. – С. 22.
6. Алиев Т.Ф. Вопросы противодействия преступлениям, совершаемым с использованием IT-технологий // Юридические исследования. 2023. № 10. С. 100-114. DOI: 10.25136/2409-7136.2023.10.44173 EDN: BDIKBI URL: https://e-notabene.ru/lr/article_44173.html
7. Вехов, В. Б. Формирование стратегий расследования преступлений на основе положений электронной криминалистики / В. Б. Вехов, П. С. Пастухов // Ex jure. –

2019. – № 4. – С. 129-141.
8. Костенко Н. С., Семененко Г. М., Пшеничкин А. А. Основные проблемы раскрытия и расследования преступлений, совершаемых с использованием информационно-телекоммуникационных технологий, на современном этапе //Вестник Воронежского института МВД России. – 2020. – №. 4. – С. 192-196.
9. Вирясова Н. В., Землянова А. Н. Проблемы раскрытия и расследования отдельных видов преступлений, совершенных с использованием информационно-телекоммуникационных технологий //Современная научная мысль, 2021. – С. 48-51.
10. Вулфел Ч. Дж. Энциклопедия банковского дела и финансов/Ч. Дж. Вулфел // ЗАО Корпорация Федоров. – Самара, 2003. – С. 1584. – ISBN 5-88833-064-7.
11. Руденко М. Б., Серебренников И. Н. Мошенничество в системах дистанционного банковского обслуживания //Научный дайджест Восточно-Сибирского института МВД России, 2019. – №. 3. – С. 189-193.
12. Нольдт С. А. Организация планирования производства следственных действий и оперативно-разыскных мероприятий по уголовному делу //Искусство правоведения. The art of law. – 2023. – №. 2 (6). – С. 67-71.
13. Бирюкова Ю.В. Проблемы, возникающие при расследовании хищений, совершенных с использованием компьютерных и телекоммуникационных технологий, и пути их решения // Вестник Московского университета МВД России, 2021. – № 4. – С. 137–142.
14. Третьякова Е.И., Бельков А.И. Перспективные направления развития технико-криминалистического обеспечения расследования мошенничеств, совершенных с использованием информационно-телекоммуникационных технологий // В сборнике: актуальные проблемы криминалистики и судебной экспертизы. Сборник материалов международной научно-практической конференции. Иркутск, 2023. – С. 139-143.
15. Шашин Д.Г. К проблеме получения оперативными подразделениями органов внутренних дел информации от кредитных организаций при выявлении, предупреждении, пресечении и раскрытии преступлений, связанных с незаконным оборотом наркотиков // Вестник Сибирского юридического института МВД России, 2019. – №2 (35). – С. 77-82.
16. Калашников К.В. Взаимодействие подразделений экономической безопасности и противодействия коррупции органов внутренних дел с банком России в ходе оперативного обслуживания кредитной сферы: проблемы и пути решения // Аграрное и земельное право, 2019. – №11 (179). – С. 152-155.
17. Гаврилин Ю.В. Практика организации взаимодействия при расследовании преступлений, совершенных с использованием информационно-коммуникационных технологий // Труды Академии управления МВД России, 2018. – №4 (48). – С. 145-150.

Результаты процедуры рецензирования статьи

В связи с политикой двойного слепого рецензирования личность рецензента не раскрывается.
Со списком рецензентов издательства можно ознакомиться здесь.

Рецензия
на статью «К вопросу взаимодействия оперативных подразделений с банковскими учреждениями по преступлениям, совершаемым с использованием информационных технологий, в том числе сети Интернет»

Представленная на рецензирование научная статья подготовлена автором на актуальную тему. Актуальность научного исследования обусловлена обстоятельствами теоретического и практического характера. Автор справедливо отмечает, что в настоящее время органам власти приходится сталкиваться со сложностями и

проблемами, возникающими в ходе внедрения информационного пространства в финансовые операции. Это привело к тому, что появились преступления нового рода, которые способствовали совершению дистанционных краж с банковских счетов путем использования новых технологических и информационных возможностей. Данная ситуация подтолкнула на создание новых коммуникационно-цифровых степеней защиты, введение в штатную численность МВД специалистов, создание отделов и управлений, занимающихся киберпреступлениями, развитие в данном направлении взаимодействия со службами безопасности банков с целью борьбы с новой угрозой. Однако в ходе таких взаимодействий возникли ряд препятствий, прежде всего отсутствие отлаженной методики взаимодействия и наличие односторонности взаимоотношений служб безопасности банков и МВД Российской Федерации при выявлении преступлений, связанных с легализацией и обналичиванием денежных средств.

Предметом исследования выступают правоотношения, возникающие в процессе взаимодействия оперативных подразделений с банковскими учреждениями по преступлениям, совершаемым с использованием информационных технологий. В исследовании поднятых проблем автор опирается на труды некоторых отечественных ученых, причем в библиографическом списке содержатся ссылки в основном на статьи опубликованные авторами по материалам научно-практических конференций. К сожалению, фундаментальные труды по данному направлению исследования в работе автора отсутствуют, что вызывает некоторое недоумение. Исследованию проблемных вопросов взаимодействия оперативных подразделений с банковскими учреждениями по преступлениям, совершаемым с использованием информационных технологий посвящены монографии и учебные пособия. Использование монографических трудов иных авторов позволило бы более глубоко проработать тему научной статьи. Далее, по тексту, автор раскрывает диспозиции норм уголовного законодательства по преступлениям совершенным посредством использования информационно-телекоммуникационных технологий, указывая лишь на кражи и мошенничество, хотя тема исследования заявлена более широко и должна охватывать иные составы преступления.

Далее, авторский переход от рассмотрения уголовно-правовой характеристики к оперативно-розыскной, также имеет некоторые неточности, которые вытекают из особенностей оперативно-розыскного законодательства. Так, автор предлагает на первоначальном этапе раскрытия преступления получить объяснение лица в отношении которого совершено преступление. Однако, ст. 6 ФЗ «Об оперативно-розыскной деятельности» предусмотрен перечень оперативно-розыскных мероприятий, которые правомочен осуществлять оперуполномоченный уголовного розыска. Так после принятия заявления от потерпевшего о совершенном преступлении может проводится комплекс ОРМ, включающий ОРМ ¬– «Опрос», в ходе которого фиксируется оперативно-значимая информация, а также иные, в том числе технические мероприятия, предусмотренные ФЗ «Об ОРД». К сожалению, в исследовании автора данные мероприятия не нашли отражение.

Далее, автор указывает на приведенный анализ оперативно-розыскной и следственной практики, научных и специальных источников, однако в научном исследовании данные направления не нашли должного отражения. Поэтому данный вопрос требует дополнительной проработки.

Кроме того, автором не были учтены в полном объеме изменения Федерального закона «О внесении изменений в статью 26 Федерального закона «О банках и банковской деятельности» и статью 27 Федерального закона «О национальной платежной системе» в части совершенствования информационного взаимодействия МВД России и Банка России по вопросам противодействия мошенничеству с платежными картами и обеспечения

информационной безопасности. Согласно Федеральному закону, на основании полученных от МВД России сведений о совершенных противоправных действиях Банк России будет предоставлять Министерству информацию о случаях и попытках переводов денежных средств, осуществленных без согласия клиента. С этой целью МВД России добавлено в состав пользователей Автоматизированной системы обработки инцидентов ФинЦЕРТ Банка России (АСОИ ФинЦЕРТ). Также между МВД России и Банком Росси заключено соглашение, регулирующее порядок информационного обмена, форму и перечень предоставляемых сведений.

Изменения в законодательство Российской Федерации вызваны большим количеством дистанционных хищений денежных средств, в том числе с использованием методов социальной инженерии. Раньше сроки рассмотрения кредитными организациями обращений правоохранительных органов по фактам такого вида мошенничества достигали 30 дней, что затрудняло проведение срочных оперативно-розыскных мероприятий и следственных действий. Теперь оперативное взаимодействие МВД России с Банком России позволит эффективно решать вопросы профилактики, пресечения и раскрытия данных преступлений.

При подготовке научного исследования автором проработаны девять источников из библиографического списка, что на наш взгляд является недостаточным для проведения репрезентативного исследования. С учетом высказанных пожеланий, работа нуждается существенной переработке.

Результаты процедуры повторного рецензирования статьи

В связи с политикой двойного слепого рецензирования личность рецензента не раскрывается.

Со списком рецензентов издательства можно ознакомиться здесь.

Предметом исследования в представленной на рецензирование статье является, как это следует из ее наименования, проблема взаимодействия оперативных подразделений с банковскими учреждениями по преступлениям, совершаемым с использованием информационных технологий, в том числе сети Интернет. Заявленные границы исследования соблюдены авторами.

Методология исследования в тексте статьи не раскрывается.

Актуальность избранной авторами темы исследования несомненна и обосновывается ими достаточно подробно: "В современных реалиях информационные технологии, в том числе информационно-телекоммуникационная сеть Интернет (далее по тексту — сеть Интернет), активно внедряются в жизнедеятельность человека и помогают ему реализовывать множество задач, например, электронное обучение, коммуникация в социальных сетях, запись к врачу через справочно-информационный интернет-портал «Госуслуги», покупки в интернет-магазинах, поиск необходимой информации в браузерах — всё это и многое другое становится возможным благодаря научно-техническому прогрессу. В настоящем исследовании автором изучены труды, в том числе монографии отечественных ученых Р. И. Дремлюга [1], А. П. Агаповой [2], В. В. Буряка [3], С.П. Бутко [4], О. А. Самсоновой [5] и др., многие из которых являются признанными учеными в области противодействия преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий (далее — ИТТ). ... Развитие информационных технологий, в частности, сказалось и на новых способах совершения киберпреступлений [6, с. 101]. К сожалению, следует констатировать тот факт, что цифровые технологии, значительно улучшая жизнедеятельность современного человека, точно так же несут в себе и потенциальную опасность для него, поскольку количество и вариативность преступлений в сфере информационных технологий (далее

– IT-преступлений) возрастают практически ежегодно. Как верно отметили В. Б. Вехов и П. С. Пастухов, «использование преступниками ИТТ в качестве средств совершения преступлений приобретает повсеместный характер, ведет к появлению новых способов совершения преступлений» [7, с. 131]".

Научная новизна работы проявляется в ряде заключений и предложений авторов: "... при получении информации о транзакциях либо о предыдущих операциях по счетам потенциального мошенника возможно провести различные ОРМ в зависимости от конкретной ситуации: 1) во-первых, путем проведения личного сыска (комплекса ОРМ, проводимых лично оперуполномоченным) «отработать» места, где производились банковские операции (предположим, продуктовые магазины). В данной ситуации оперативный сотрудник посещает подобные локации, просматривает при соответствующем запросе видеокамеры на установление изображения злоумышленника, далее проводит ОРМ «Опрос» в отношении сотрудников магазинов, их владельцев, посетителей на предмет того, видели ли они данное лица, как часто они видят его, какие особые приметы они могут выделить, родственные и иные связи, возможные пути следования, какие дополнительные данные об изучаемом лице могут предоставить и т. д.; 2) во-вторых, с наличием конкретной информации оперативный сотрудник путем проведения ОРМ «Наблюдение» проверяет возможные маршруты потенциального мошенника: в каком направлении он направился (при просмотре записи видеокамер), какие продуктовые магазины имеются рядом; также путем ОРМ «Опрос» стоит установить контакт с местными жильцами, с так называемыми старшими по дому, чтобы уточнить оперативно-значимую информацию о данном лице, проживало или проживает и как давно, как часто появляется, с кем живёт, контактные данные лица и т. д." и др.; "Принимая во внимание тот факт, что действия сотрудников оперативных подразделений полиции по направлению запросов в кредитные организации обусловлены выполнением возложенных на них обязанностей по выявлению, предупреждению, пресечению и раскрытию преступлений, а также тот факт, что указанные действия соответствуют правам сотрудников ОВД, предоставление информации, отнесенной к профессиональной тайне, по запросам полиции не может быть расценено как ее разглашение"; "Изменения в законодательство Российской Федерации вызваны большим количеством дистанционных хищений денежных средств, в том числе с использованием методов социальной инженерии. Несомненно, оперативное взаимодействие МВД России с Банком России позволит эффективно решать вопросы профилактики, пресечения и раскрытия данных преступлений. Однако при этом вышеназванным законом не был урегулирован срок предоставления указанных сведений оперативным подразделениям" и др. Таким образом, статья вносит определенный вклад в развитие отечественной правовой науки и, безусловно, заслуживает внимания потенциальных читателей.

Научный стиль исследования выдержан авторами в полной мере.

Структура работы вполне логична. Во вводной части статьи ученые обосновывают актуальность избранной им темы исследования. В основной части работы авторы исследуют некоторые аспекты взаимодействия оперативных подразделений с банковскими учреждениями по преступлениям, совершаемым с использованием информационных технологий, в том числе сети Интернет, выявляют соответствующие проблемы и предлагают пути их решения. В заключительной части статьи содержатся выводы по результатам проведенного исследования.

Содержание статьи соответствует ее наименованию, но не лишено недостатков формального характера.

Так, авторы пишут: "Несомненно, безналичный вид расчёт становится всё более востребованным для общества, но в то же время необходимо сказать и о различных способах завладения безналичных денежных средств" - "расчетов"; "безналичными

денежными средствами".

Ученые отмечают: "Метод кражи безналичных денег при помощи скримминга с карты в копировании данных магнитной ленты банковской карты, а затем создание её копии, чтобы позже снять с неё деньги" - предложение не согласовано.

Таким образом, статья нуждается в дополнительном вычитывании - в ней встречаются опечатки и стилистические ошибки (приведенный в рецензии перечень опечаток и ошибок не является исчерпывающим!).

Библиография исследования представлена 17 источниками (диссертационной работой, монографиями, научными статьями). С формальной и фактической точек зрения этого достаточно. Авторам удалось раскрыть тему исследования с необходимой глубиной и полнотой.

Апелляция к оппонентам имеется, но носит общий характер в силу направленности исследования. Научная дискуссия ведется авторами корректно; положения работы обоснованы в должной степени и проиллюстрированы примерами.

Выводы по результатам проведенного исследования имеются ("С учётом вышеизложенного и принимая во внимание отсутствие законодательного закрепления сроков предоставления оперативно-значимой информации от банковских учреждений, авторы статьи полагают целесообразным дополнить статью 8 Федерального закона «Об оперативно-розыскной деятельности» от 12 августа 1995 г. № 144-ФЗ следующим содержанием: «В рамках проведения оперативно-розыскного мероприятия „Наведение справок“ по преступлениям, совершаемым с использованием информационных технологий, в том числе сети Интернет, оперативные подразделения по направляемым запросам в банковские учреждения делают отметку о необходимости предоставления обратного ответа в течение 72 часов с целью своевременного выявления и раскрытия данной категории преступлений и установления причастных к ним лиц, в том числе их местонахождения». Несомненно, оперативным подразделениям как носителям профессиональной информации, т. е. не подлежащей разглашению, и, помимо этого, с целью более эффективного и своевременного выявления и раскрытия преступлений, совершаемых с использованием сети Интернет, видится важным закрепление на законодательном уровне сроков предоставления сведений оперативным сотрудникам от банковских учреждений"), обладают свойствами достоверности, обоснованности и, безусловно, заслуживают внимания научного сообщества, но не отражают всех научных достижений авторов статьи. Следовательно, они нуждаются в уточнении и конкретизации.

Интерес читательской аудитории к представленной на рецензирование статье может быть проявлен прежде всего со стороны специалистов в сфере уголовного процесса и криминалистики при условии ее доработки: раскрытии методологии исследования, уточнении и конкретизации выводов по его результатам, устранении нарушений в оформлении работы.

Результаты процедуры окончательного рецензирования статьи

В связи с политикой двойного слепого рецензирования личность рецензента не раскрывается.

Со списком рецензентов издательства можно ознакомиться здесь.

Предмет исследования. В рецензируемой статье «К вопросу взаимодействия оперативных подразделений с банковскими учреждениями по преступлениям, совершаемым с использованием информационных технологий, в том числе сети Интернет» предметом исследования являются нормы права, регулирующие общественные отношения в сфере взаимодействия правоохранительных органов и

финансово-кредитных учреждений по выявлению и расследованию правонарушений (преступлений) с применением информационно-коммуникационных технологий, в том числе посредством глобальной сети Интернет.

Методология исследования. В ходе написания статьи использовались современные методы исследования: общенаучные и частные. Методологический аппарат составили следующие диалектические приемы научного познания: абстрагирование, индукция, дедукция, гипотеза, аналогия, синтез, а также можно отметить применение типологии, классификации, систематизации и обобщения.

Актуальность исследования. Актуальность темы статьи не вызывает сомнения, поскольку существуют юридические и фактические проблемы выявления и расследования преступлений с применением информационно-коммуникационных технологий в банковской сфере, в том числе с использованием возможностей сети Интернет. Особо остро стоит вопрос о взаимодействии банковских учреждений с оперативными подразделениями правоохранительных органов. Как правильно отмечают авторы статьи, «…противодействие преступлениям с использованием ИТТ становится для правоохранительных органов едва ли не первоочередной задачей в их повседневной деятельности». Неоднозначность и противоречивость правовых норм в данной сфере общественных отношений и их официального толкования требует дополнительных доктринальных разработок по данной проблематике с целью совершенствования современного уголовного законодательства и правоприменения.

Научная новизна. Не подвергая сомнению важность проведенных ранее научных исследований, послуживших теоретической базой для данной работы, тем не менее, можно отметить, что и в этой статье тоже сформулированы некоторые заслуживающие внимания положения, которые имеет характер научной новизны, например: «Несомненно, оперативным подразделениям как носителям профессиональной информации, т. е. не подлежащей разглашению, и, помимо этого, с целью более эффективного и своевременного выявления и раскрытия преступлений, совершаемых с использованием сети Интернет, видится важным закрепление на законодательном уровне сроков предоставления сведений оперативным сотрудникам от банковских учреждений». Разработанные авторами предложения по совершенствованию законодательства можно расценивать как практическую значимость данного исследования.

Стиль, структура, содержание. Статья написана научным стилем с использованием специальной юридической терминологии. Содержание статьи соответствует ее названию, хотя на взгляд рецензента, название статьи слишком «громоздкое». Соблюдены требованию по объему статьи. Статья логически структурирована, но формально не разделена на части. Материал изложен последовательно, грамотно и ясно. Замечаний по содержанию нет.

Библиография. Авторами использовано достаточное количество доктринальных источников, есть ссылки на публикации последних лет. Ссылки на источники оформлены с соблюдением требований библиографического ГОСТа.

Апелляция к оппонентам. В статье представлена научная полемика. Обращения к оппонентам корректные, оформлены ссылками на источники опубликования.

Выводы, интерес читательской аудитории. Представленная на рецензирование статья «К вопросу взаимодействия оперативных подразделений с банковскими учреждениями по преступлениям, совершаемым с использованием информационных технологий, в том числе сети Интернет» может быть рекомендована к опубликованию. Статья написана на актуальную тему, отличается научной новизной и практической значимостью. Публикация по данной теме могла бы представлять интерес для читательской аудитории, прежде всего, специалистов в области уголовного права, а также, могла бы быть

полезна для преподавателей и обучающихся юридических вузов и факультетов.