Всероссийский институт повышения квалификации
сотрудников Министерства внутренних дел Российской Федерации

ПОРЯДОК ДЕЙСТВИЙ СОТРУДНИКОВ ОРГАНОВ ВНУТРЕННИХ ДЕЛ ПО РАСКРЫТИЮ И РАССЛЕДОВАНИЮ ХИЩЕНИЙ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Методические рекомендации

Домодедово
ВИПК МВД России
2021

ББК 67.408.135
П 60

Авторский коллектив:

Ю. Н. Гришин – начальник кафедры ОРД ОВД ВИПК МВД России, полковник полиции;

К. А. Сергеев – старший преподаватель кафедры ОРД ОВД ВИПК МВД России, майор полиции;

Н. В. Мурзин – начальник отдела по раскрытию преступлений, совершаемых с использованием ИТТ УУР УМВД России по Ивановской области, подполковник полиции;

Б. Г. Кулиш – старший оперуполномоченный 4 отделения ОУР УВД по СВАО ГУ МВД России по г. Москве старший лейтенант полиции.

Рецензенты:

К. Ю. Строганов – начальник УВД по СВАО ГУ МВД России по г. Москве, полковник полиции;

А. М. Уразметов – врио заместителя начальника полиции (по оперативной работе) УВД по СВАО ГУ МВД России по г. Москве, полковник полиции;

К. В. Фролов – начальник кафедры профессиональной деятельности сотрудников подразделений экономической безопасности Нижегородской академии МВД России, подполковник полиции.

П 60 **Порядок действий сотрудников органов внутренних дел по раскрытию и расследованию хищений, совершенных с использованием информационно-телекоммуникационных технологий** : методические рекомендации / Ю. Н. Гришин, К. А. Сергеев, Н. В. Мурзин, Б. Г. Кулиш. – Домодедово: ВИПК МВД России, 2021. – 42 с.

В методических рекомендациях представлен алгоритм действий сотрудников оперативных подразделений территориальных органов по оперативному сопровождению расследования уголовных дел, возбужденных по фактам киберхищений, в том числе относящихся к категории небольшой и средней тяжести.

Методические рекомендации предназначены для слушателей, студентов, курсантов, аспирантов, профессорско-преподавательского состава образовательных организаций МВД России, а также сотрудников оперативных подразделений, следствия, дознания и дежурных частей, имеющих различный опыт работы и уровень профессиональной подготовки.

ОГЛАВЛЕНИЕ

ОСНОВНЫЕ ПОНЯТИЯ, ОПРЕДЕЛЕНИЯ И АББРЕВИАТУРЫ

Дроп – лицо, предназначенное для промежуточного приема товаров/банковских переводов/посылок/и т.д.

Дроп карта – карта, оформленная на подставное лицо, предназначенная для промежуточного приема банковских переводов, наличных денежных средств.

Киберхищение – хищение, совершенное дистанционным способом с использованием информационно-телекоммуникационных технологий[1].

Оперативное сопровождение расследования уголовных дел по киберхищениям – основанная на законе и ведомственных нормативных правовых актах МВД России деятельность оперативных подразделений органов внутренних дел[2] по проведению комплекса оперативно-розыскных мероприятий и иных законных действии, проводимых на основании наличия уголовных дел и направленных на установление лиц, совершивших киберхищение, а также непрерывное своевременное и полное обеспечение предварительного следствия информацией, содержащей совокупность фактических данных об обстоятельствах преступного деяния и фактах противодействия ему.

Абонентский номер – номер, идентифицирующий оконечный элемент сотовой связи. Он состоит из 11 последовательных цифр, 1-я из которых определяет код страны, 2, 3, 4-я определяют принадлежность абонентского номера к региону или оператору сотовой связи, остальные – определяющий номер клиента.

IMEI – уникальный номер сотового аппарата. Данный номер состоит из 15 последовательных цифр, из которых первые 14 определяют происхождение, модель и серийные номер сотового устройства, а 15-я – контрольная цифра.

Интернет-сайт – совокупность страниц, объединенных одной тематикой, дизайном, а также взаимосвязанной системой ссылок. Каждая страница может содержать в себе видео- и фотоизображения, аудиофайлы, рекламные блоки и много другое.

---

[1] Далее – ИТТ.
[2] Далее – ОВД.

IP-адрес – это уникальный идентификационный номер, который присваивается каждому компьютеру при выходе в сеть Интернет. Он представляет собой последовательность из 4 цифр в диапазоне от 0 до 255, чередующихся через точку. Например, 178.218.36.0. IP-адрес выдается компьютеру его интернет провайдером в момент начала Интернет-сессии – открытия первой Интернет-страницы, и заканчивается закрытием Интернет-сессии – закрытием последней Интернет-страницы.

Хостинг (англ. hosting) – услуга по предоставлению ресурсов для размещения информации на сервере, постоянно имеющем доступ к сети (обычно Интернет).

Доменное имя – символьное обозначение, следующее за обозначением всемирной сети («www»). К примеру, «vk.com», «youtube.com», «2ip.ru» и др.

БИН банка – банковский идентификационный номер. Это первые шесть цифр номера банковской карты.

Электронный кошелек (англ. e-Purse или e-Wallet) – смарт-карта или другой электронный носитель со встроенным чипом, позволяющий хранить электронные деньги и осуществлять различные платежи.

SIP-телефония – это связь через интернет с помощью протокола передачи данных SIP, который расшифровывается как Session Initiation Protocol – протокол установления сеанса.

Протокол установления сеанса SIP – протокол передачи данных, описывающий способ установки и завершения пользовательского Интернет-сеанса, включающего обмен мультимедийным содержимым (IP-телефония, видео- и аудиоконференции, мгновенные сообщения, онлайн-игры).

Виртуальный номер – телефонный номер, не привязанный к определенному телефонному устройству или телефонной линии, работающий в сети Интернет.

Cookie-файл – это фрагмент данных, который Интернет-сайт передает в Интернет-браузер (Google Chrome, Mozilla Firefox и др.) своего нового пользователя, чтобы «запомнить» его.

Интернет-прова́йдер (от англ. internet service provider, сокр. ISP – поставщик Интернет-услуги) – организация, предоставляющая услуги доступа к сети Интернет и иные связанные с Интернетом услуги.

VPN (в переводе с англ. – виртуальная частная сеть) – обобщенное название технологий, позволяющих обеспечить одно или несколько соединений поверх другой сети. Иными словами при использовании VPN устройство принимает участие в виртуальной частной сети с несколькими пользователями, получая случайный IP-адрес, при этом их трафик неотличим друг от друга, так же в такой сети обеспечивается криптографическая защита.

MAC-адрес – физический адрес устройства, является статическим, присваивается всем видам устройств от мобильных телефонов до персональных компьютеров.

Сетевая плата (сетевая карта) – дополнительное устройство, позволяющее персональному компьютеру иметь доступ к сети и взаимодействовать с другими устройствами. Существуют интегрированные в материнскую плату с урезанным функционалом и отдельные устройства. Как правило, для совершения преступлений используется именно отдельное устройство, так как интегрированная карта легко устанавливается в ходе оперативно-технического мероприятия[1].

Роутер – специализированный компьютер, пересылающий пакеты данных между различными сегментами сети на основе таблицы и правил маршрутизации.

Прокси (англ. proxy) – звено посредник между устройством, которое использует абонент, и системой Интернет-серверов. Иначе говоря, это удаленный компьютер-посредник для выхода в интернет под чужим MAC и IP-адресом.

SIM-банк (свитч) – VoIP GSM шлюзы пользуются растущей популярностью среди российских компаний, предпринимателей и мошенников. В связи с возможностью горячей замены / установки SIM-карт; а также автоматическим распределением SIM-карт между GSM шлюзами по временным правилам и автоматической заменой SIM-карт на

[1] Далее – ОТМ.

GSM шлюзах при наступлении определенных событий или по временным критериям. Что затрудняет проведение ОТМ, так как номер, с которого мошенник производил звонок, может быть деактивирован в короткие сроки. В таких случаях необходимо установить MAC-адрес и IMEI-адрес устройства.

Глава 1. ОРГАНИЗАЦИОННЫЕ МЕРОПРИЯТИЯ

При раскрытии и расследовании хищений, совершаемых с использованием информационно-телекоммуникационных технологий, на заместителя начальника территориального органа МВД России на региональном уровне – начальника Следственного управления, начальников следственных подразделений территориальных органов МВД России на районном уровне при проведении организационно-штатных мероприятий возлагаются обязанности по внесению изменений в составы специализированных следственно-оперативных групп подразделений территориальных органов по раскрытию и расследованию хищений, совершенных с использованием информационно-телекоммуникационных технологий.

Начальник УУР территориального органа МВД России на региональном уровне возлагает на сотрудников УУР территориального органа МВД России на региональном уровне, несущих службу в составе следственно-оперативной группы УМВД, обязанности по координации взаимодействия сотрудников следственно-оперативных групп территориальных органов МВД России на районном уровне с ПСТМ, ООРИ и ДЧ территориального органа МВД России на региональном уровне.

Начальник отдела по раскрытию преступлений, совершаемых с использованием информационно-телекоммуникационных технологий УУР территориального органа МВД России на региональном уровне обязан ежедневно контролировать работу территориальных органов МВД России на районном уровне по раскрытию хищений, совершенных с использованием информационно-телекоммуникационных технологий.

Начальник подразделения ОРИ территориального органа МВД России на региональном уровне по согласованию должен предоставлять в УУР территориального органа МВД России на региональном уровне сведения о результатах оперативно-аналитических мероприятий, в том числе при взаимодействии с подразделениями ООРИ территориальных органов МВД России на региональном уровне других

субъектов Российской Федерации, в отношении лиц, возможно причастных к совершению преступлений рассматриваемого вида.

Руководители (начальники) территориальных органов МВД России на районном уровне:

Организовывают незамедлительное рассмотрение заявлений, обращений граждан о хищениях, совершенных с использованием ИТТ, с обязательным задействованием сотрудников уголовного розыска и следственных подразделений, закрепленных за данным направлением работы.

При наличии достаточных данных, указывающих на признаки состава преступления, не требующих дополнительной проверки, принимают меры по возбуждению по фактам хищений, совершенных с использованием ИТТ, уголовных дел в течение суток, обеспечив при этом подготовку и направление в соответствующие подразделения и организации (ИЦ территориального органа МВД России на региональном уровне, подразделения уголовного розыска, банки, суды) по компетенции следующих документов:

1) статистической карты формы № 1.0 на выявленное преступление с заполненными реквизитами 26 и 26.1;

2) согласованного плана следственных действий и оперативно-розыскных мероприятий, учитывающего обстоятельства совершения преступления;

3) согласованных с руководителем следственного органа или органа дознания запросов на получение информации о движении денежных средств по счетам потерпевшего (подозреваемого) в порядке, предусмотренном статьей 26 Федерального закона от 2 декабря 1990 г. № 395-1 «О банках и банковской деятельности» (см. приложение № 1);

4) ходатайства в суд о получении информации о соединениях между абонентами и (или) абонентскими устройствами в порядке, предусмотренном статьями 165, 186.1 Уголовно-процессуального кодекса Российской Федерации (см. приложение № 2);

5) отдельного поручения в подразделение уголовного розыска, содержащего сведения, необходимые для заведения дела оперативного учета и проведения оперативно-розыскных мероприятий;

6) при совершении хищений с использованием сотовой связи или IP-телефонии – запросов в компании, представляющие услуги связи (см. Приложение № 3).

Доследственные проверки по заявлениям, сообщениям (обращениям) граждан о хищениях, совершенных с использованием ИТТ, рекомендуется проводить в кратчайшие сроки, но не более 10 суток.

Внесение информации о совершенных с использованием ИТТ хищениях в ИБД-Ф «Дистанционное мошенничество» и в оперативную сводку о происшествиях, преступлениях на обслуживаемой территории (сервис обеспечения деятельности дежурных частей ИСОД МВД России) необходимо осуществлять оперативно.

Глава 2. АЛГОРИТМ ДЕЙСТВИЙ СОТРУДНИКОВ ПРИ ПОЛУЧЕНИИ ЗАЯВЛЕНИЙ (СООБЩЕНИЙ) О КИБЕРХИЩЕНИИ

Алгоритм действий сотрудников дежурных частей при получении заявления (сообщения) о киберхищении:

Сообщения и заявления о преступлениях, вне зависимости от времени и места их совершения, а также полноты содержащихся в них сведений и формы представления подлежат обязательному приему во всех территориальных органах МВД России.

При обращении в дежурную часть органа внутренних дел граждан с сообщением или заявлением о готовящемся, совершаемом или совершенном мошенничестве, оперативный дежурный обязан:

1. Принять и зарегистрировать заявление, сообщение в соответствии с нормативными правовыми актами, регламентирующими порядок приема, регистрации и разрешения в ОВД Российской Федерации заявлений, сообщении и иной информации о преступлениях и происшествиях.

2. Выяснить у заявителя данные:

- о времени, месте, способе и обстоятельствах совершения мошеннических действий;

- информацию о номерах расчетных счетов, откуда и куда были переведены денежные средства, а также каким способом (через платежный терминал, банкомат, банковским переводом (через оператора банковского учреждения путем составления банковского поручения), электронные платежные системы, с карты на карту и т.д.);

- об Интернет-ресурсах, с помощью которых было совершено преступление (сайты, социальные сети);

- сведения о предполагаемом преступнике (как представлялся, какие данные о себе сообщил, номера телефонов, электронной почты, паспортные и иные данные, акцент, характерные особенности речи);

- значительность причиненного ущерба для потерпевшего (с учетом его материального положения);

- иную информацию, имеющую значение для дальнейшего раскрытия преступления.

3. С учетом полученной первичной информации, а также исходя из характера совершенного преступления, определить состав следственно-оперативной группы, при необходимости обеспечить участие в осмотре места происшествия специалистов-криминалистов и иных специалистов, организовать выезд следственно-оперативной группы и обеспечить сотрудников средствами связи, криминалистической техникой и транспортом для доставления к месту происшествия и обратно.

4. Заносить данные о дистанционных мошенничествах в базу, согласно приказу МВД России от 22.04.2020 № 236 «О вводе в эксплуатацию подсистемы «Дистанционное мошенничество» ПТК «ИБД-Ф».

Алгоритм действий следственно-оперативной группы по прибытию на место происшествия:

1. Незамедлительно провести осмотр мобильного устройства, персонального компьютера или иных технических средств, используемых потерпевшим в период совершения преступления, с целью установления данных подозреваемого (реквизиты банковского счета, ФИО лица, кому переведены денежные средства, время и сумма перевода и т.д.), а также поиска электронных документов, имеющих отношение к уголовному делу (сделать скриншоты или фото выполненных транзакций).

2. Организовать получение у оператора сотовой связи детализации абонентских соединений, производимых по номеру телефона потерпевшего, за интересующий период времени. С целью оперативности получения данных сведений рекомендуется личное обращение потерпевшего в службу поддержки оператора или через личный кабинет абонента.

3. Организовать получение расширенной справки-выписки за сутки по банковской карте, с которой произошло хищение денежных средств, используя приложение на техническом устройстве потерпевшего по его личному обращению или звонку в службу поддержки банка.

4. В случаях, если денежные переводы осуществлялись посредством перевода на счёт через банкомат, необходимо зафиксировать момент

перевода посредством снятия видеозаписи с камеры видеонаблюдения помещения, в котором расположен банкомат.

Алгоритм действий сотрудников оперативных подразделений при получении заявления (сообщения) о киберхищении:

1. Сотрудник оперативного подразделения при непосредственном обращении гражданина принимает заявление, получает от него объяснение и собирает информацию о киберхищении:

- время, место, способ и обстоятельства совершения мошеннических действий;

- информацию о номерах расчетных счетов, откуда и куда были переведены денежные средства (место открытия счета потерпевшего), а также каким способом (через платежный терминал, банкомат, банковским переводом (через оператора банковского учреждения путем составления банковского поручения), электронные платежные системы, с карты на карту и т.д.);

- об Интернет-ресурсах, с помощью которых было совершено преступление (сайты, социальные сети);

- сведения о предполагаемом преступнике (как представлялся, какие данные о себе сообщил, номера телефонов, электронной почты, паспортные и иные данные, акцент, характерные особенности речи);

- значительность причиненного ущерба для потерпевшего (с учетом его материального положения);

- иную информацию, имеющую значение для дальнейшего раскрытия преступления.

2. В соответствии с частью 1 статьи 144 УПК РФ исполняет письменные поручения следователя (дознавателя) о проведении оперативно-розыскных мероприятий в установленный законом срок.

3. В случаях, если преступление совершенно с использованием мобильного телефона, с целью получения предполагаемых данных лица, совершившего преступление, необходимо получить информацию об абонентском номере, использованном при совершении преступления.

С помощью сайта Федерального агентства связи (Россвязь)[1] или сайта телефонных кодов городов России, кодов стран мира, кодов сотовых операторов (def-коды)[2] и иных сайтов установить принадлежность оператору и региону данного абонентского номера.

4. Направляет запрос оператору сотовой связи о предоставлении сведений о пользователе данного абонентского номера (Ф.И.О. абонента, дата рождения, адрес регистрации, паспортные данные, их копия) (см. приложение № 4)

5. Проводит оперативно-розыскные мероприятия, направленные на получение образцов голоса подозреваемого лица. Для этого может быть использовано любое техническое средство для записи телефонных разговоров, состоящее на балансе органа внутренних дел, в том числе имеющееся в его распоряжении, либо заявителя. Например, телефон с установленной программой (диктофон) для записи переговоров.

Сотрудник оперативного подразделения докладывает рапортом о проведенных мероприятиях руководителю органа внутренних дел и принимает меры к сохранению полученной аудиозаписи для последующего приобщения к материалам уголовного дела.

6. Информацию о банковском счете, на который были перечислены похищенные денежные средства, можно получить из платежных документов, предоставленных заявителем, или из выписки о движении денежных средств по счету, которую заявитель лично может получить в банке обслуживания счета.

При подготовке постановлений и запросов необходимо иметь в виду, что номер банковской карты не совпадает с номером расчетного счета, к которому она «привязана». По первым 6 цифрам (bin), указанным в номере банковской карты, можно определить, каким кредитным учреждением выдана банковская карта[3].

7. Устанавливает место обналичивания похищенных денежных средств: подготавливает постановление о ходатайстве перед судом о

[1] URL: http : www. rossvyaz.ru/activity/num_resurs/registerNum/ (дата обращения: 20.09.2021).
[2] URL: http: www.kody.su (дата обращения: 20.09.2021).
[3] URL: https://www.bindb.com/bin-database.html (дата обращения: 14.09.2021).

получении разрешения на проведение ОРМ «Наведение справок» в кредитной организации с целью получения сведений о владельце счета, движении денежных средств по нему за интересующий период, мест снятия денежных средств, а также снятие записей с камер видеонаблюдения с банкомата и находящихся в непосредственной близости, на которых может быть запечатлен подозреваемый.

8. В случаях, если совершение преступления совершено с использованием фишингового сайта (сайта зеркала), необходимо установить полное название ресурса (доменного имени). В данном случае необходимо провести осмотр места происшествия, а именно технического устройства потерпевшего с целью фиксации истории браузера. Отличительные черты данных сайтов – имитация названий оригинального ресурса (Vk9.com; Av1to.ru; ula.ura).

9. Направить запрос на сайт Reg.ru для уточнения данных о владельце сайта зеркала, а также IP-адреса сервера или устройства, используемого при совершении преступления, и его местонахождении (геолокации) (см. приложение № 5).

10. В случаях использования оригинального ресурса (сайта), на котором расположена заведомо ложная информация, стоит учитывать, что оплата товара на таком сайте происходит исключительно через онлайн систему, встроенную в его структуру. В большинстве случаев злоумышленники выводят беседу с потерпевшими в мессенджеры, такие как Whatsapp, Telegram, Viber, используя подложные номера. При этом стоит учитывать, что запрос на используемый номер, направляемый в ПСТМ для определения принадлежности, носит информационный характер.

В подобных случаях необходимо проведение детализации и анализа Интернет-трафика, так как наличие IMEI номера устройства злоумышленника позволит впоследствии проводить оперативно-технические мероприятия непосредственно по устройству, используемому лицом, совершающим мошеннические действия. Анализ интернет трафика позволит установить посещаемые злоумышленником Интернет-ресурсы и его связи по средствам мессенджеров.

11. Отправленная злоумышленником ссылка на оплату может свидетельствовать о наличии зарегистрированной на его имя онлайн-кассы. Для установления данных лица, на чье имя зарегистрирована данная онлайн-касса, а также наличия привязанного к ней расчётного счёта и юридического адреса необходимо направить запрос в Федеральную налоговую службу (см. приложение № 6)

12. В случаях, если злоумышленник передал номер электронного кошелька (QIWI, Яндекс, WEBMONY, МОБИ деньги и др.) для денежного перевода, необходимо подготовить постановление о ходатайстве перед судом о получении разрешения на проведение ОРМ «Наведение справок» с целью получения информации о принадлежности электронного кошелька, движения денежных средств по нему, связанные с ним постоянными переводами иные электронные кошельки, устройства, используемые для авторизации на ресурсе, а также получения их IP-адресов с указанием времени, данными расчетных счетов и номеров банковских карт получателей.

Распространены случаи подмены номера посредством создания SIM-карты дубликата.

Так, мошенник, злоупотребляя доверием потерпевшего (в ходе личного знакомства или посредством телефонного звонка, представляясь сотрудником силовых структур либо службы безопасности банка), узнаёт номер и паспортные данные, привязанные к карте потерпевшего.

Далее, используя связи с сотрудниками коммерческих фирм, а именно банков, узнаёт кодовое слово, привязанное к карте с целью получения доступа к счёту.

После чего преступник посредством личных контактов перевыпускает SIM-карту потерпевшего с идентичным абонентским номером и паспортными данными. Впоследствии совершает звонок в службу поддержки банка, представляясь потерпевшим. В ходе беседы с сотрудниками банка злоумышленник осуществляет замену пин-кода, используя кодовое слово, а также цифровой пароль, который приходит на подменный номер.

13. В данном случае необходимо осуществить следующие мероприятия:

13.1. Отследить маршрут денежных средств, выведенных со счёта, путем направления запроса в банк, используемым потерпевшим (см. приложение № 7).

13.2. Провести ОРМ СИТКС по абонентскому номеру, с целью получения информации об устройстве (его виде, IMEI номере, mac-адресе). В ходе анализа СИТКС имеется возможность установления местонахождения (геопозиции) предполагаемого злоумышленника, а также времени совершения им преступления.

В том числе при анализе данных будет установлено место первой активации перевыпущенной SIM-карты (салон связи). Таким образом, имеется возможность установления лица, заказавшего данную SIM-карту (снятие изображение с видеокамер, установленных в салоне связи либо в непосредственной близости, проведение опроса работников данного салона связи).

14. Направить запрос мобильному оператору потерпевшего для уточнения места перевыпуска SIM-карты с целью установления лица, совершившего данную операцию без присутствия владельца номера (см. приложение № 8).

15. Направить запрос в банк, используемый потерпевшим, с целью получения образца голоса злоумышленника, звонившего на линию поддержки клиентов и представившегося владельцем банковской карты, который забыл пин-код от нее и код авторизации мобильного сервиса банка (см. приложение № 9).

15.1. В случаях, если преступник совершил преступление, использовав социальные сети (вконтакте, одноклассники, мой мир и др.), необходимо подготовить постановление о ходатайстве перед судом о получении разрешения на проведение ОРМ «Наведение справок», с целью получения информации о владельце профиля, привязанный к аккаунту абонентский номер, IP-адреса авторизации (см. приложение № 10).

16. При получении сведений вышеуказанных сведений, сотрудник оперативного подразделения осуществляет их проверку по ИБД-Ф модуль поиска «дистанционные мошенничества», с целью установления принадлежности абонентского номера, банковской карты, онлайн-

кошелька, имя которым представлялись, на интернет ресурсе, торговой площадке, социальной сети.

16.1. Проводит иные оперативно-розыскные мероприятия, направленные на установление личности подозреваемого и последующего его задержания.

Алгоритм действий следователей и дознавателей при получении заявления (сообщения) о киберхищении:

1. При проведении проверки по сообщению о киберхищении, рекомендуются проводить следующие действия:

1.1. Получить объяснение от заявителя. В ходе опроса отразить выяснить следующие сведения:

– в какое время, каком месте и при каких обстоятельствах произошло общение с лицом, совершившем мошеннические действия;

– каким образом данное лицо привлекло внимание заявителя (что он говорил потерпевшему; какая ситуация была смоделирована); зафиксировать подробности состоявшегося разговора, а также особенности разговора и речи (используемые выражения, наличие акцента, дефекты речи) преступника; присутствовал ли кто-либо при этом разговоре;

– в чем выражался обман и почему заявитель передал денежные средства или иное имущество; отразить обстоятельства передачи или перевода денежных средств;

– какие действия подозреваемого или его слова сформировали доверительное отношение заявителя;

– производились ли заявителем какие-либо записи в ходе контакта с подозреваемым, получались ли электронные образы документов;

– кто мог быть очевидцем преступления, возможный адрес их нахождения;

– является ли ущерб значительным для заявителя, если да, то обязательно отразить обстоятельства, подтверждающие это (состав семьи, близких родственников, лиц, находящихся на иждивении, размер доходов и расходов заявителя);

– что именно заявитель сообщил преступнику, кем представлялся звонивший (родственником, сотрудником полиции, банка и т.п.);

– в случае использования посредника (курьера, таксиста и т.п.): через какой период времени после окончания разговора подъехал неизвестный к дому заявителя; описание голоса неизвестного лица (курьера, таксиста), какие особенности, странности в интонации, произношении звуков, в обращении к нему он заметил; по каким приметам заявитель сможет опознать его голос; подробное описание его черт лица, рук, особенностей телосложения, походки, поведения, по которым заявитель сможет его опознать (составить композиционный портрет личности), одежды; если передача денег осуществлялась в жилище заявителя, установить: когда неизвестный курьер (таксист) зашел в квартиру, до каких предметов мебели, иных предметов дотрагивался, как себя вел, что сообщил, задавал ли какие-либо вопросы, задавал ли заявитель ему какие-либо вопросы, интересовался ли судьбой своего родственника, например, путем постановки вопроса, когда родственника «освободят» от уголовной ответственности и пр.; сообщал ли заявитель неизвестному точную сумму денег, которую передал ему, для каких целей он передает ему эти деньги; судя по поведению неизвестного, был ли тот осведомлен о содержимом, переданном ему, о причинах (целях) передачи ему денежных средств; пересчитывал ли заявитель, неизвестное лицо на месте передачи деньги; как заявитель упаковал деньги; звонил ли неизвестный в момент получения денег кому-либо, что говорил; провожал ли заявитель неизвестного, наблюдал ли за направлением, в котором неизвестный покинул место расположения его дома, передвигался ли неизвестный на автомобиле (какой модели); какую сумму денег он хранит дома.

1.2. При осуществлении безадресного перевода, необходимо выяснить, на чье имя переводились деньги, полные установочные данные получателя, истребовать у заявителя квитанцию о переводе. Если перевод был осуществлен на лицевой счет абонентского номера или счет банковской карты, необходимо выяснить:

– абонентский номер телефона или номер банковской карты, с которой переведены денежные средства (дата получения, срок действия, вид платежной системы, банк-эмитент карты, наличие договора банковского счета и документов об оформлении банковской карты), истребовать данные документы, чек или квитанцию о переводе;

– абонентский номер телефона или номер банковской карты, на которую переведены денежные средства;

– размер суммы перевода денежных средств;

– предпринятые заявителем действия после обнаружения факта мошеннических действий;

1.3. В ходе получения объяснения от потерпевшего при проверке факта дистанционного хищения, совершенного с использованием сети Интернет, необходимо установить:

– дату и время обнаружения объявления (получения ссылки на соответствующий Интернет-ресурс);

– при помощи какого технического устройства потерпевший выходил на сайт с размещенным объявлением (переходил по Интернет-ссылке);

– какие характеристики продаваемого товара были указаны в объявлении о продаже;

– какие условия купли-продажи содержались в объявлении (условия о предоплате, оплате товара, сроках и видах его поставки, ответственности сторон);

– какие контактные данные продавца были указаны в объявлении о продаже;

– имелись ли отзывы, комментарии к объявлению о продаже;

– сохранились ли у него данные объявления (№ объявления, ID-страницы);

– каким образом, когда (дата, время) заявитель связался с продавцом;

– как представился продавец;

– отразить подробное содержание разговора с продавцом;

– описать голос продавца, установить, сможет или нет его опознать (по каким приметам);

– когда, каким образом (через банкомат, посредством услуги «Сбербанк Онлайн», «Мобильный банк»), в каком размере заявитель перечислил денежные средства в счет оплаты за якобы приобретаемый товар, а также на какой счет был осуществлен перевод (номер счета либо банковской карты, открытые на чье имя);

– если перевод денежных средств заявитель осуществил со своей банковской карты на банковскую карту неизвестного посредством услуги «Сбербанк Онлайн», через «Личный кабинет», то установить место входа потерпевшего в сеть Интернет (с какого компьютера, ноутбука, планшета, с использованием какого модема, wi-fi роутера, их MAC-адреса, логины и пароли, какая компания-провайдер предоставляла в этот день заявителю услуги доступа в Интернет).

2. В целях сокращения времени проведения проверки следователю (дознавателю) необходимо истребовать у потерпевшего документы на банковское обслуживание карты, со счета которой произошло списание денежных средств, а также иных документов, подтверждающих факт перевода денежных средств на другие банковские карты (счета) или лицевой счет абонентского номера. Данные сведения потерпевший может получить самостоятельно при помощи личного кабинета в мобильном приложении.

3. После возбуждения уголовного дела с согласия руководителя следственного органа следователю необходимо запросить полные сведения об осуществленном переводе по коду транзакции. Либо, получив судебное решение, следователь (дознаватель) производит выемку документов, содержащих информацию о счетах граждан в банках и иных кредитных организациях.

Следует отметить, что информация о соединениях между абонентами и абонентскими устройствами, движении денежных средств по счету SIM-карты, IMEI номере устройства, в котором использовались SIM-карты с интересующими следствие абонентскими номерами, следователем (дознавателем) может быть получена в порядке, установленном статьями 165 и 186.1 УПК РФ и после возбуждения уголовного дела.

В соответствии с частью 4 статьи 26 Федерального закона от 02.12.1990 № 395-1 «О банках и банковской деятельности» справки по счетам и вкладам физических лиц могут быть выданы кредитной организацией без судебного решения по согласованным с руководителем следственного органа запросам следователя только по уголовным делам, находящимся в его производстве, но не при проведении проверки сообщения о преступлении. При этом, дознаватель не включен в перечень

должностных лиц, правомочных запрашивать в кредитных организациях сведения о вкладах и счетах физических лиц, операциях и счетах юридических лиц и граждан, осуществляющих предпринимательскую деятельность без образования юридического лица, определенный статьей 26 указанного Федерального закона. Дознаватели при производстве расследования по уголовному делу получают данную банковскую информацию только по решению суда.

Такой же порядок определен и при необходимости получения информации о движении денежных средств по лицевому счету абонентского номера, банковскому счету, посредством определенной платежной системы, о пользователях, совершивших соответствующие операции. Так, согласно статьи 26 Федерального закона от 27.06.2011 №161-ФЗ (ред. от 27.06.2018) «О национальной платежной системе» операторы по переводу денежных средств, операторы платежных систем, операторы услуг платежной инфраструктуры и банковские платежные агенты (субагенты) обязаны гарантировать банковскую тайну в соответствии с законодательством Российской Федерации о банках и банковской деятельности.

Поэтому, в случае необходимости получения вышеуказанных сведений от операторов сотовой связи, кредитной организации или администрации платежной системы при проверке сообщения о преступлении следователю (дознавателю) следует использовать полномочия оперативных подразделений органов внутренних дел, предоставленные последним в соответствии с Федеральным законом от 12.08.1995 № 144-ФЗ (ред. от 06.07.2016) «Об оперативно-розыскной деятельности» и Федеральным законом от 07.07.2003 № 126-ФЗ (ред. от 03.08.2018) «О связи».

4. До возбуждения уголовного дела, либо в ходе его расследования следователь (дознаватель) должен направить запрос в организацию, обслуживающую Интернет-ресурс, на котором подозреваемый в совершении мошенничества, разместил объявление о продаже товара (предоставлении услуг и пр.).

5. После получения сведений об IP-адресах, следователю (дознавателю) необходимо направить запросы провайдерам, которыми

были присвоены такие IP-адреса с целью установления данных клиента, которому присвоен IP-адрес, а также адреса местонахождения конечного оборудования (точки доступа в сеть Интернет), с приложением заверенных копий документов (договора) об оказании услуг связи.

6. В случае необходимости получения информации о владельце электронной почты (о регистрации и администрировании) @gmail.com (@google.com), @hotmail.com, @yahoo.com (и прочие) необходимо учитывать, что указанные компании находятся на оборудовании организаций, осуществляющих свою деятельность за пределами Российской Федерации. Таким образом, получить вышеуказанные сведения возможно посредством направления запроса по линии НЦБ Интерпола, либо запроса о правовой помощи в соответствии со статьями 453 и 454 УПК РФ после возбуждения уголовного дела[1].

7. В случае поступления от оператора сотовой связи (организации, обслуживающей Интернет-ресурс) информации об абонентах, достоверность паспортных данных которых вызывает сомнение, необходимо направить запрос в соответствующее территориальное подразделение Управления по вопросам миграции МВД России по субъекту РФ с целью проверки этих данных.

7.1. Рекомендуется получать данную информацию от исполнителей запросов сначала посредством электронной почты для организации своевременного проведения необходимых процессуальных и следственных действий, а затем - оригинал получать почтой или иным способом.

8. При совершении операций по банковской карте через устройство самообслуживания (банкомат), следователю (дознавателю) необходимо направить запрос в соответствующую организацию с просьбой об архивации видеозаписи с камер наблюдения. Данные видеозаписи в ходе проведения проверки сообщения о преступлении необходимо изъять при

[1] Порядок направления запросов, сообщений, следственных поручений и ответов по линии Интерпола определен Инструкцией по организации информационного обеспечения сотрудничества по линии Интерпола, утвержденной приказом МВД России, Минюста России, ФСБ России, ФСО России, ФСКН России, ФТС РФ от 06.10.2006 № 786/310/470/454/333/971 (ред. от 22.09.2009) «Об утверждении Инструкции по организации информационного обеспечения сотрудничества по линии Интерпола» // Бюллетень нормативных актов федеральных органов исполнительной власти. № 47. 20.11.2006.

проведении осмотра места происшествия или после возбуждения уголовного дела в порядке, установленном статьей 183 УПК РФ.

9. При проверке заявления (сообщения) о преступлении осмотр места происшествия может проводиться до возбуждения уголовного дела.

На момент получения сообщения о киберхищении, как правило, может быть известно:

– место нахождения заявителя в момент преступления;

– место перевода (зачисления и т.п.) денежных средств.

Если способ совершения дистанционного хищения заключался в размещении на соответствующем Интернет-ресурсе информации о продаже товаров (оказании услуг) без намерения выполнять свои обязательства, а заявитель просмотрел такое объявление с помощью технического средства (компьютер, ноутбук, планшет, wi-fi роутер, модем и пр.), расположенного в занимаемом им жилом помещении, то осмотр места происшествия (жилища заявителя) проводится с его согласия.

Осмотр места происшествия производится с целью фиксации обстановки, обнаружения и изъятия следов в виде электронной информации, предметов – носителей такой информации, иных предметов и документов, которые могут иметь значение для раскрытия и расследования преступления.

В случае, если Интернет-ресурс, с использованием которого совершены противоправные действия, продолжает функционировать на момент осмотра места происшествия (не удален, не заблокирован и т.п.), необходимо в протоколе указать представленную на сайте контактную информацию, род деятельности ресурса, наличие отзывов, приложить распечатки с Интернет-сайта, экранную копию (скриншот экрана) ресурса сети Интернет, на которой указаны реквизиты – адресная строка страницы, идентификатор страницы и т.д.

В ходе осмотра места происшествия могут быть изъяты системные блоки персональных компьютеров или установленные в них накопители на жестких магнитных дисках, иные электронные носители информации, которые могут иметь значение для раскрытия и расследования преступления.

В рамках осмотра места происшествия следователем (дознавателем) с письменного согласия заявителя также может быть проведен осмотр его мобильного телефона. Такой осмотр целесообразно проводить с участием специалиста.

В рамках осмотра необходимо детально исследовать соответствующие разделы приложения «Мобильный банк» («История платежей», «Последние операции» и пр.), в которых зафиксировано движение денежных средств по счету (банковской карте), сделать снимки экрана (скриншоты) мобильного устройства, либо сфотографировать экран любым устройством, позволяющим получить фотографическое изображение. Обнаружению и закреплению (фотографированию) также подлежит информация, находящаяся в памяти мобильного устройства, отражающая переписку с лицом, осуществившем преступление.

Информация, полученная в ходе осмотра мобильного устройства, подлежит занесению протокол, а фотоматериалы необходимо приобщить в виде фототаблицы.

В ходе проведения осмотра места происшествия, также возможно изъятие, полученных самостоятельно заявителем, документов и сведений, относящихся к событию хищения (детализации собственного абонентского номера; выписки движения денежных средств по банковской карте (счету), с которого были переведены денежные средства; договор банковского счета (банковского обслуживания), а также документов об оформлении банковской карты (заявления на открытие банковского счета и предоставление банковской расчетной карты) и др.).

Для перевода денежных средств как на лицевой счет абонентского номера

При проверке сообщения (заявления) о преступлении следователем (дознавателем) в соответствии с частью 1 статьи 144 УПК РФ могут быть осмотрены все обнаруженные и изъятые при производстве осмотра места происшествия или истребованные предметы и документы.

Осмотр компьютерных устройств, электронных носителей информации и, мобильных телефонных аппаратов и их содержимого, видеозаписей, документов и др. может являться составной частью осмотра места происшествия. Как самостоятельное же следственное действие он

производится в тех случаях, когда в ходе осмотра места происшествия обнаруженные и изъятые предметы и документы, имеющие значение для дела, не были сразу осмотрены, или, когда возникает необходимость в повторном их осмотре, требуется длительное время для более детального изучения, применение специальных знаний и технических средств.

10. В случае, когда хищение денежных средств осуществлялось путем неправомерного вмешательства в функционирование компьютерных устройств или информационно-телекоммуникационных сетей, обязательным условием при принятии решения о возбуждении уголовного дела является установление способа совершения данного вида мошенничества. Для чего необходимо располагать заключением эксперта (судебной компьютерной экспертизы).

При назначении компьютерной экспертизы средств сотовой связи (мобильного телефона, смартфона, планшетного компьютера, оборудованного слотом для использования SIM-карты (модуль идентификации абонента) перед экспертом могут быть поставлены вопросы, позволяющие:

– установить номер IMEI (международный идентификатор мобильного оборудования, состоящий из 15 цифр) телефона (смартфона, планшетного компьютера) в привязке к SIM-карте, установленной в данном устройстве (при регистрации устройства в сотовой сети происходит привязка информации оператора связи, содержащаяся на SIM-карте к IMEI устройства, позволяющий идентифицировать владельца SIM-карты (абонента), по номеру IMEI устройства, и наоборот, информация привязки «SIM-карта-IMEI» позволяет установить все IMEI номера устройств, работавших в паре с данной SIM);

– определить и скопировать всю содержащуюся в памяти устройства информацию (номера из абонентской книжки, СМС-сообщения, последние набранные номера, входящие вызовы, фото-, видеофайлы и пр.);

– определить и скопировать информацию из чатов (переписка с помощью мгновенных сообщений (WhatsApp, Viber), как текстовых, так и пересылаемых фото и видео файлов), по содержанию которых можно установить обстоятельства совершения преступления.

Вопросы, которые могут быть поставлены перед экспертом, конкретизируются с учетом объектов исследований и складывающейся следственной ситуации.

11. Следователь (дознаватель) в ходе предварительной проверки вправе давать органу дознания обязательное для исполнения письменное поручение о проведении оперативно-розыскных мероприятий, о производстве отдельных следственных и иных процессуальных действий (пункт 4 части 2 статьи 38, пункт 1.1 части 3 статьи 41, часть 1 статьи 144 УПК РФ).

Поручение о производстве оперативно-розыскных мероприятий исполняется в срок до 10 суток. Результаты выполнения поручения о проведении оперативно-розыскных мероприятий могут быть доложены начальнику органа дознания рапортом, после чего приобщаются следователем (дознавателем) к материалу проверки либо уголовному делу.

Глава 3. ОРГАНИЗАЦИЯ ПРОФИЛАКТИЧЕСКИХ МЕРОПРИЯТИЙ

Профилактические мероприятия осуществляются на постоянной основе и направлены на решение комплексных проблем. К основным профилактическим мероприятиям относятся:

1. Анализ преступлений, совершённых с использованием информационно-телекоммуникационных технологий с целью выявления тенденции их развития и выработки мероприятий по их пресечению, выявлению и раскрытию.

2. Организация профилактических бесед с гражданами на территории оперативного обслуживания, при этом уделяя особое внимание «группам риска» – пожилые люди и несовершеннолетние.

3. Путем звукового оповещения в общественных местах проводить информирование граждан о преступных схемах в сфере информационно-телекоммуникационных технологий и способах противодействия.

4. Разработка, изготовление и распространение памяток с разъяснением возможных мошеннических действий.

5. Проведение рабочих встреч с представителями организаций банковской сферы, операторов сотовой связи, экспертных компаний в области IT – индустрии и иных заинтересованных лиц, с целью выработки совместных действий, направленных на противодействие преступлениям в сфере информационно-телекоммуникационных технологий.

6. Проведение межведомственных рабочих встреч, семинаров и совещаний с целью организации совместных действий по выявлению, пресечению, раскрытию и расследованию киберхищений.

7. Освещение в средствах массовой информации, а также сети Интернет о способах совершения преступных действий в сфере информационно-телекоммуникационных технологий, а также методах противодействия.

ЛИТЕРАТУРА

1. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ. – Доступ из справочной правовой системы «КонсультантПлюс».

2. Об оперативно-розыскной деятельности : Федеральный закон от 12.08.1995 № 144-ФЗ. – Доступ из справочной правовой системы «КонсультантПлюс».

3. О внесении изменений в Федеральный закон «О связи» : Федеральный закон от 30.12.2020 № 533-ФЗ. – Доступ из справочной правовой системы «КонсультантПлюс».

4. О деятельности органов внутренних дел по предупреждению преступлений : приказ МВД России от 17 января 2006 г. № 19. – Специализированная территориально распределенная автоматизированная система СТРАС «Юрист».

5. О полиции : Федеральный закон от 7 февраля 2011 г. № 3-ФЗ (с изм. и доп.). – Доступ из справочной правовой системы «КонсультантПлюс».

6. О связи : Федеральный закон от 07.07.2003 № 126-ФЗ. – Доступ из справочной правовой системы «КонсультантПлюс».

7. Об утверждении Инструкции о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд : приказ МВД России, Минобороны России, ФСБ России, ФСО России, ФТС России, СВР России, ФСИН России, ФСКН России, СК России от 27 сентября 2013 г. № 776/703/509/507/1820/42/535/398/68. – Специализированная территориально распределенная автоматизированная система СТРАС «Юрист».

8. Об утверждении Инструкции по организации информационного обеспечения сотрудничества по линии Интерпола : приказ МВД России, Минюста России, ФСБ России, ФСО России, ФСКН России, ФТС РФ от 06.10.2006 № 786/310/470/454/333/971 (ред. от 22.09.2009) // Бюллетень нормативных актов федеральных органов исполнительной власти. – 2006. – № 47.

9. Олиндер, Н.В. Преступления, совершенные с использованием электронных платежных средств и систем: криминалистический аспект: монография / Н. В. Олиндер. – Москва: Русайс, 2016. – 124 с.

10. Русскевич, Е.А. Уголовное право и «цифровая преступность»: проблемы и решения : монография / Е. А. Русскевич. – Москва: ИНФРА-М, 2020. – 227 с. – (Научная мысль). – DOI 10.12737/monography_5bcdb21e969119.61135230.

11. Русскевич, Е. А. Уголовно-правовое противодействие преступеиям, совершаемым с спользованием информационно-коммуникционных технологий : учебное пособие / Е. А. Русскевич. – Москва: ИНФРА-М, 2017. – 115 с. – (Высшее образование: Магистратура). – DOI 10.12737/24712.

ПРИЛОЖЕНИЯ

Приложение № 1

Угловой штамп
территориального органа
МВД России

Директору Управления
Начальнику службы
безопасности
наименование банка

« ____ » _____ 20 г. № _____
на № _____ от _____

О направлении запроса

В связи с расследованием уголовного дела № 12001450030000514, возбужденного 17 января 2021 года по признакам состава преступления, предусмотренного по п. "г" ч. 3 ст. 158 УК РФ, прошу предоставить расширенную выписку по движению денежных средств по банковским картам ПАО «**Банк**» № **** **** **** ****.

В связи с тем, что банковская карта могла быть использована злоумышленниками в целях получения денежных средств, просим Вас предоставить сведения о местах обналичивания денежных средств с данных банковских карт, предоставить расширенные выписки по движениям денежных средств за 07.01.2021, информацию по проведенным платежам, с временными отметками и отражением дальнейшего движения денежных средств, IP-адресах, используемых в банке клиента (за указанный период времени), мобильные телефоны, а также любую значимую информацию, представляющую оперативный интерес по данному уголовному делу.

В случае возникновения вопросов по факту исполнения запроса, прошу Вас связаться с оперуполномоченным УУР УМВД А.А. Ивановым по телефону: 8 901 000 00 00.

Начальник А. А. Смирнов

Приложение № 2

П О С Т А Н О В Л Е Н И Е
о возбуждении перед судом ходатайства о проведении оперативно-розыскного мероприятия «Наведение справок»

г. Домодедово «_ _» _____ 2021 г.

Начальник УМВД России по г.о. Домодедово А.А. Иванов, рассмотрев материалы дела в отношении неустановленного лица (установленного лица),

У С Т А Н О В И Л:

Сотрудниками УУР УМВД России по г.о. Домодедово проводятся оперативно-розыскные мероприятия, направленные на установление причастности *неустановленного лица (установленного лица)* к совершению преступлений, связанных с хищениями денежных средств мошенническим путем с использованием мобильной связи и сети Интернет.

В ходе проведения оперативно-розыскных мероприятий установлено, что *лицо, совершающее хищение денежных средств мошенническим путем,* для связи использует мобильный телефон: 8 901 000 00 00.

Таким образом, в действиях *неустановленного лица (установленного лица)* усматриваются признаки преступления, предусмотренного ч. 4 ст. 159 УК РФ.

С целью проверки сведений о противоправной деятельности *неустановленного лица (установленного лица)* необходимо провести оперативно-розыскное мероприятие «Наведение справок».

Предусмотренных законом обстоятельств, препятствующих проведению оперативно-розыскного мероприятия, не имеется.

На основании изложенного, руководствуясь ст. 23 Конституции РФ и ст. 1, 2, 3, 5 ч. 1, 6, 7, 8 Федерального закона от 12.08.1995 № 144-ФЗ «Об оперативно-розыскной деятельности», с последующими изменениями, внесенными федеральными законами РФ,

П О С Т А Н О В И Л:

Обратится в Домодедовский городской суд Московской области за разрешением на проведение оперативно-розыскного мероприятия «Наведение справок».

Начальник А. А. Иванов

Приложение № 3

ООО «Наименование оператора IP-телефонии»
электронная почта организации

Угловой штамп
территориального органа
МВД России

_____ № _____
на № _____ от _____

О предоставлении информации

В соответствии с п. 3, 4 ст. 13 Федерального закона «О полиции» и ч. 3 ст. 26, ч. 4 ст. 26 Федерального закона «О связи» в рамках осуществления функций по выявлению, предупреждению и пресечению преступлений прошу Вас в срок, не позднее трех рабочих дней от даты получения запроса, представить в **территориальный орган МВД России** всю имеющуюся информацию в отношении пользователя, использующего абонентский номер 8 499 999 999, а именно:

- информацию о паспортных данных, поданных при заключении договора о предоставлении услуг;
- информацию об использованных для заключения договора абонентских номерах и электронных почтах;
- информацию о том, каким образом была произведена регистрация пользователя;
- информацию об IP-адресах, использованных для входа в личный кабинет, а также в панель управления по администрированию данным абонентским номером;
- информацию об оплате услуг, с указанием полных реквизитов плательщика;
- статистику звонков с 01.10.2020 года по настоящее время;
- информацию об абонентских номерах, на которые поступала переадресация звонков.

В связи со срочностью получения запрашиваемой информации прошу Вас предоставить ответ на служебную почту sotrudnik@mvd.ru.

В случае необходимости разъяснения истребуемой информации просим связаться с исполнителем.

Начальник А. А. Иванов

Исполнитель: П.П. Петров
Тел.: 8 901 000 000 00

Приложение № 4

Угловой штамп
территориального органа
МВД России

Генеральному директору
ООО «Мобильный оператор»
ФИО

_____ № _____
на №_____от_____

О предоставлении информации

В связи со служебной необходимостью, а также необходимостью получения фактической информации, имеющей значение для решения задач в оперативно-розыскной деятельности, направленной на выявление, предупреждение и пресечение преступлений, на основании п. 2 ч. 1 ст. 6 Федерального закона от 12.08.1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности», просим Вас предоставить в **территориальный орган МВД России** информацию о абонентском номере телефона 8 901 000 00 00.

Неповиновение законному распоряжению или требованию сотрудника полиции, а равно воспрепятствование исполнению им служебных обязанностей влечет за собой административную ответственность, предусмотренную статьей 19.3 Кодекса Российской Федерации об административных правонарушениях.

Непредставление или несвоевременное представление в государственный орган (должностному лицу) сведений (информации), представление которых предусмотрено законом и необходимо для осуществление этим органом (должностным лицом) его законной деятельности, а равно представление в государственный орган (должностному лицу) таких сведений (информации) в неполном объеме или в искаженном виде, за исключением случаев, предусмотренных статьями 19.8, 19.19 Кодекса Российской Федерации об административных правонарушениях, влечет за собой административную ответственность, предусмотренную статьей 19.7 Кодекса Российской Федерации об административных правонарушениях.

Начальник А. А. Иванов

исп: П.П. Петров
тел: 8 (495) 955 955 55

Приложение № 5

Исполнительному директору
ООО «Регистратор Доменных
имен Рег.Ру»

А.В. Колову

125467, г. Москва, ул. Василия
Петушкова, д.3, стр.1
84955140573
info@reg.ru
pravo@support.reg.ru

Угловой штамп
территориального органа
МВД России

_____ № _____
на № _____ от _____

О предоставлении информации

В соответствии с п. 3, 4 ст. 13 Федерального закона «О полиции» и ч. 3 ст. 26, ч. 4 ст. 26 Федерального Закона «О связи», в рамках осуществления функций по выявлению, предупреждению и пресечению преступлений, прошу Вас в срок, не позднее трех рабочих дней от даты получения запроса, представить в **территориальный орган МВД России** всю имеющуюся информацию в отношении пользователя polzovatel.ru.

- информацию о паспортных данных регистратора доменного имени;
- информацию об использованных для регистрации абонентских номерах и электронных почтах;
- информацию о том, каким образом была произведена регистрация пользователя;
- информацию об IP-адресах, использованных для входа в личный кабинет или панель управления для администрирования доменного имени;
- информацию об оплате услуг регистрации и аренды доменного имени, с указанием полных реквизитов плательщика;
- аналогичную информацию по иным доменным именам, зарегистрированным данным пользователем, установленным при анализе Cookie-файлов.

В связи со срочностью получения запрашиваемой информации, прошу Вас предоставить ответ на служебную почту sotrudnik@mvd.ru.

В необходимости разъяснения истребуемой информации просим связаться с исполнителем – оперуполномоченным П. П. Петровым.

Начальник А. А. Иванов

Исп.: П. П. Петров
8-901-000-00-0
sotrudnik@mvd.ru

Приложение № 6

Угловой штамп
территориального органа
МВД России

В ФНС (ИФНС)
адрес подразделения

_____ № _____
на №_____от_____

О предоставлении информации

В связи с осуществлением функций по выявлению, предупреждению и пресечению экономических, налоговых и коррупционных преступлений, на основании ст. 12 Федерального закона от 07.02.2011 № 3-ФЗ «О полиции», руководствуясь п. 4 ч. 1 ст. 10, п. 4 ч. 1 ст. 13 Федерального закона от 07.02.2011 № 3-ФЗ «О полиции», ст. 6 Федерального закона «Об оперативно-розыскной деятельности», в соответствии с Соглашением о взаимодействии между МВД России и ФНС России от 13.10.2010 № 1/8656, ММВ-27-4/11, а также проведением проверки (КУСП № ____ от 01.01.2021), прошу Вас представить в наш адрес следующие сведения (заверенные копии документов) в отношении «Наименование организации, ИНН» за период с 01.01.2021 по настоящее время:

- документы регистрационного дела налогоплательщика;
- сведения об открытых (закрытых) расчетных счетах;
- сведения по форме 2-НДФЛ;
- расширенную выписку из ЕГРЮЛ (с паспортными данными руководителей и учредителей).

Начальник А. А. Иванов

исп: П. П. Петров
тел: 8(495)955 955 55

Приложение № 7

Угловой штамп
территориального органа
МВД России

Начальнику службы
безопасности
Банковской организации

_____№ _____
на №_____ от _____

О предоставлении информации

В связи с расследованием уголовного дела № 1234571384373, возбужденного 01 января 2021 года, по признакам состава преступления, предусмотренного по ч. 4 ст. 159 УК РФ, прошу предоставить документированную информацию (заверенные копии документов) в отношении **ИНН/КПП**, по всем расчетным счетам (открытым, закрытым), за период с момента открытия счета по настоящее время:

1. Справки по имеющимся счетам указанного юридического/физического лица за весь период.
2. Расширенную справку (выписку) о движении денежных средств с указанием получателя (отправителя) платежа, его реквизитов, суммы платежа, назначении платежа и даты операции по следующей форме:

Дата	Номер документа	Корсчет	БИК	Счет	Наимен. контрагента	ИНН\ КПП	Дебет	Кредит	Назначен. платежа

3. Установочные данные на генерального директора и главного бухгалтера, адрес фактического местонахождения организации, контактные телефоны, а также данные о лицах, действующих по доверенности от имени указанной организации при заключении договора банковского счета (расчетно-кассового обслуживания), закрытии расчетного счета (копию юридического дела указанной организации).
4. Доверенности на получение выписок со счетов и актов о признании электронной подписи с момента открытия счетов и по настоящее время, а также информацию об **IP-адресах** клиента, с которых осуществлялся вход и управление по системе «клиент-банк»;
5. Сведения о сомнительных ИНН/КПП, выявленных в соответствии с правилами внутреннего контроля, в порядке, предусмотренном Федеральным законом от 07.08.2001 №115-ФЗ «О противодействии

легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», за весь период деятельности.

В случае возникновения вопросов по факту исполнения, вы можете связаться непосредственно с исполнителем – оперуполномоченным ОУР П. П. Петровым по телефону: 8 495 000 00 00.

Начальник А. А. Иванов

исп: П. П. Петров
тел: 8(495) 000 00 00

Приложение № 8

Угловой штамп
территориального органа
МВД России

_____ № _____
на № _____ от _____

ООО «Компания,
предоставляющая услуги связи»
электронная почта

О предоставлении информации

В соответствии с п. 3, 4 ст. 13 Федерального закона «О полиции» и ч. 3 ст. 26, ч. 4 ст. 26 Федерального закона «О связи», в рамках осуществления функций по выявлению, предупреждению и пресечению преступлений, прошу Вас в срок, не позднее трех рабочих дней от даты получения запроса, представить в **территориальный орган МВД России** всю имеющуюся информацию в отношении пользователя, использующего абонентский номер 84992130419, а именно:

- информацию о паспортных данных, поданных при заключении договора о предоставлении услуг;
- информацию о том, каким образом была произведена регистрация пользователя;
- информацию об оплате услуг, с указанием полных реквизитов плательщика;
- информация о физическом перевыпуске данной сим-карты, а именно организацию осуществившую данное действие, её юридический адрес.

В связи со срочностью получения запрашиваемой информации, прошу Вас предоставить ответ на служебную почту sotrudnik@mvd.ru.

В необходимости разъяснения истребуемой информации просим связаться с исполнителем – оперуполномоченным ОУР П. П. Петровым.

Начальник А. А. Иванов

исп.: П. П. Петров
тел.: 8 (495) 000 00 00

Приложение № 9

Руководителю ПАО
«Банковская организация»

Угловой штамп
территориального органа
МВД России

_____ № _____
на № _____ от _____

О предоставлении информации

В связи с расследованием уголовного дела № 12001450030000514, возбужденного 01 января 2021 года, по признакам состава преступления, предусмотренного по п. «г» ч. 3 ст. 158 УК РФ, прошу предоставить запись телефонного звонка, совершённого с номера 8 499 987 89 00 в центр клиентской поддержки.

В связи с тем, что банковская карта могла быть использована злоумышленниками в целях получения денежных средств, просим Вас предоставить запись телефонного разговора, а также предоставить расширенные выписки по движениям денежных средств за 01.01.2021, информацию по проведенным платежам, с временными отметками и отражением дальнейшего движения денежных средств, IP-адресах, используемых в банке клиента (за указанный период времени), иные мобильные телефоны, а также любую значимую информацию, представляющую оперативный интерес по данному уголовному делу.

В случае возникновения вопросов по факту исполнения, Вы можете связаться непосредственно с исполнителем – оперуполномоченным ОУР П. П. Петровым по телефону: 8 499 010 0000.

Начальник А. А. Иванов

исп.: П. П. Петров
тел.: 8 (495) 000 00 00

Приложение № 10

Угловой штамп
территориального органа
МВД России

Руководителю службы
безопасности
ООО «Социальная сеть»

_____
Адрес организации

_____№ _____
на №_____ от _____

О предоставлении информации

В связи с проведением проверки по факту совершения противоправных действий неустановленными лицами (КУСП № _____ от 01.01.2021), на основании п. 4 ч. 1 ст. 13 Федерального закона от 07.02.2011 № 3-ФЗ «О полиции», п. 2 ч. 1 ст. 6 и ст. 7 Федерального закона от 12.08.1995 № 144-ФЗ «Об оперативно-розыскной деятельности», а также ст. 64 Федерального закона от 07.07.2003 №126-ФЗ «О связи», прошу Вас предоставить в наш адрес всю имеющуюся информацию (IP-адреса регистрации и авторизации, электронные почтовые ящики, абонентские номера, персональные данные, указанные пользователем при регистрации) по учетной записи: ссылка на профиль.

В случае возникновения вопросов по факту исполнения, Вы можете связаться непосредственно с исполнителем – оперуполномоченным ОУР П. П. Петровым по телефону:8 495 000 00 00

Начальник А. А. Иванов

исп.: П. П. Петров
тел.: 8 (495) 000 00 00

Учебное издание

Гришин Юрий Николаевич,

Сергеев Кирилл Александрович,

Мурзин Николай Вадимович,

Кулиш Борис Григорьевич

ПОРЯДОК ДЕЙСТВИЙ СОТРУДНИКОВ ОРГАНОВ ВНУТРЕННИХ ДЕЛ ПО РАСКРЫТИЮ И РАССЛЕДОВАНИЮ ХИЩЕНИЙ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Редактор, технический редактор: И.В. Карась

Подписано в печать 10.12.2021. Формат 60х84 1/16. Объем 2,0 уч.-изд. л.
Тираж 50 экз. Заказ 44/21. Цена договорная.

Федеральное государственное казенное учреждение дополнительного профессионального образования «Всероссийский институт повышения квалификации сотрудников Министерства внутренних дел Российской Федерации»
Ул. Пихтовая, д. 3, мкр. Авиационный, г. Домодедово,
Московская обл., 142007