



**Управление Министерства Внутренних дел Российской  
Федерации по Тамбовской области**

**Управление уголовного розыска**

*Методические рекомендации: «Основы раскрытия и  
расследования мошеннических действий, совершенных с  
использованием средств сотовой связи и сети интернет»*



**«МОБИЛЬНЫЕ МОШЕННИКИ»**

г. Тамбов, 2018 год

## Оглавление:

Введение	3
1. Общие сведения и понятия	
1.1 Понятие сотовой связи и базовых станций	4
1.2 Понятие абонентского номера	4
1.3 Понятие IMEI	6
1.4 Понятие IP-адреса и средства анонимизации в сети (VPN)	7
1.5 Ресурсы, используемые для хранения и перевода денежных средств	9
1.6 Понятие интернет сайта. Схема получения информации	12
1.7 SIP-телефония. Звонки через интернет	14
1.8 Понятие Cookie-файлов, как средство деанонимизации в сети	15
2. Сведения, представляющие интерес для раскрытия и расследования уголовного дела	
2.1 Сведения, которые необходимо запрашивать у сотовых операторов	18
2.2 Сведения, которые необходимо запрашивать по банковским карта и расчетным счетам	18
2.3 Сведения, которые необходимо запрашивать по электронным кошелькам	19
2.4 Сведения, которые необходимо запрашивать по сайтам объявлений	20
2.5 Сведения, которые необходимо запрашивать по социальным сетям	21
2.6 Сведения, которые необходимо запрашивать по доменному имени сайта	21
2.7 Сведения, которые необходимо запрашивать по хостингу сайта	22
2.8 Сведения, которые необходимо запрашивать по IP-адресу	22
2.9 Сведения, которые необходимо запрашивать по электронной почте	22
2.10 Сведения, которые необходимо запрашивать у SIP-провайдера	23
3. Схемы расследования наиболее распространённых телефонных и интернет мошенничеств	
3.1 Схема №1. Мошенничество, совершенное через сайты объявлений. Мошенник-продавец	24
3.2 Схема №2. Мошенничество, совершенное через сайты объявления. Мошенник-покупатель	25
3.3 Схема №3. Мошенничество со взломом страниц социальной сети	26
3.4 Схема №4. Мошенничество, совершенное с использованием интернет сайтов	27
3.5 Схема №5. Мошенничество, совершенное под предлогом заказа банкета	28
3.6 Схема №6. Мошенничество, совершенное под предлогом совершения операций по банковским картам	29
3.7 Схема №7. Мошенничество, совершенное под предлогом помощи родственнику, попавшему в беду	30
3.8 Схема №8. Мошенничество, совершенное под предлогом компенсации за ранее приобретенные БАДы (биологически активные добавки).	31
3.9 Схема №9. Мошенничество, совершенное с использованием вредоносных программ на ОС «Android»	32
3.10 Схема №10. Мошенничество, совершенное с использованием социальных сетей (интернет магазин «Вконтакте»)	33
Заключение	34

## Введение






Телефонное мошенничество — один из самых распространённых видов преступной деятельности в наше время. Начиная с 2015 года наблюдается ежегодный рост количества совершенных преступлений указанной категории, вот почему так остро стоит вопрос об ответных мерах реагирования со стороны правоохранительных органов.

Данные методические рекомендации разработаны с целью обучения сотрудников органов внутренних дел методам и алгоритмам раскрытия и расследования преступлений по линии телефонного мошенничества, а также направлены на ориентирование сотрудников к творческому и индивидуальному подходу при работе с каждым преступлением.

Сами по себе алгоритмы и схемы расследования мошеннических действий, совершенных с использованием средств сотовой связи и сети интернет, не дадут положительного результата, если сотрудник не имеет представления о запрашиваемой им информации. Указанное обстоятельство предопределило структуру построения настоящих методических рекомендаций:

1. Общие сведения о ресурсах, используемых мошенником.
2. Сведения, получаемые сотрудником по указанным ресурсам и имеющие существенное значение для раскрытия и расследования уголовного дела.
3. Схема возможных вариантов использования полученных сведений.

Стоит отметить, что настоящие методические рекомендации могут быть использованы и в иных оперативных и следственных целях:

-  Для установления места фактического жительства лиц, представляющих оперативный интерес.
-  Для розыска преступников и без вести пропавших.
-  Для установления сбытчиков похищенного (при продаже на «Авито», «Юле» и других сайтах).
-  Для установления лиц, причастных к незаконному обороту наркотических средств.
-  Для установления лиц, причастных к распространению нацистской символики в сети интернет.

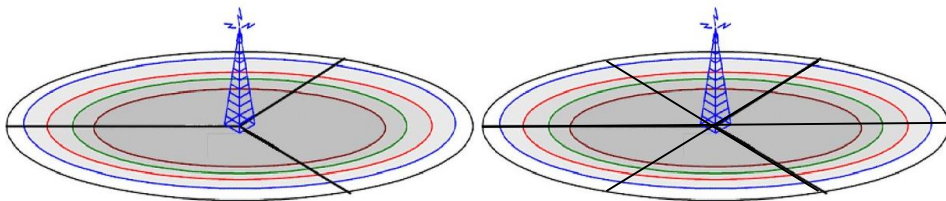
# 1. ОБЩИЕ СВЕДЕНИЯ И ПОНЯТИЯ

## 1.1 Понятие сотовой связи и базовых станций

Большинство схем дистанционных мошеннических действий основаны на использовании средств радиосвязи.

Одним из самых распространенных видов радиосвязи является «Сотовая связь». Ее также называют «Сеть подвижной связи», так как она предоставляет свои услуги без использования кабеля. Ключевая особенность «Сотовой связи» заключается в том, что общая зона покрытия делится на ячейки (секторы), определяющиеся зонами покрытия отдельных базовых станций – комплекса приемопередающей аппаратуры, которая обслуживает абонентов в своей зоне действия.

Базовые станции устанавливают на крышах высоких зданий, а также вышках, и делят зону их покрытия на три или шесть секторов:



Базовые станции могут покрывать территорию от 0,5 км до 15 км вокруг места установки. При этом, чем выше плотность населения, тем ближе к друг другу их располагают – в черте города они могут располагаться даже на расстоянии 100 метров друг от друга, в сельской же местности – 10-15 км.

**В этой связи представляется целесообразным запрашивать у оператора сотовой связи наряду с детализацией телефонных разговоров и информацию о характеристиках используемых базовых станций с указанием азимута их действия, количества секторов (антенных блоков). Указанная информация поможет определить узкий сектор, в котором может проживать мошенник.**

Аналогичным способом по уголовному делу №11801680033000113 (ОД ОП №2 УМВД России по г. Тамбову) был установлен адрес съемного жилья злоумышленника, а именно с использованием анализа показателей базовой станции.

## 1.2 Понятие абонентского номера

Под «абонентским номером» следует понимать – номер, идентифицирующий окончательный элемент сотовой связи. Он состоит из 11 последовательных цифр, 1-ая из которых определяет код страны,

2,3,4-ая определяют принадлежность абонентского номера к региону или оператору сотовой связи, остальные – определяющий номер клиента.

Для установления принадлежности абонентского номера к тому или иному сотовому оператору необходимо получить выписку из ресурса нумерации «Федерального агентства связи», который находится в открытом доступе на сайте [www.rossvyaz.ru](http://www.rossvyaz.ru) (прямая ссылка: [www.rossvyaz.ru/activity/num\\_resurs/registerNum](http://www.rossvyaz.ru/activity/num_resurs/registerNum)).

К примеру, необходимо установить принадлежность абонентского номера 8-900-123-45-67, на сайте это выглядит следующим образом:

**Выписка из реестра Российской системы и плана нумерации**  
**Результат поиска**

Код   
пример: 495

Номер\*

Оператор



**Найдено записей: 1**



Код	Диапазон	Емкость	Оператор	Регион
900	1200000 - 1399999	200000	ООО "Т2 Мобайл"	Ростовская обл.





*Установлено, что абонентский номер 8-900-123-45-67 принадлежит оператору сотовой связи «Теле2» в Ростовской области.*







Самыми распространенными сотовыми операторами являются «Мобильные ТелеСистемы» (МТС), «Т2 Мобайл» (Теле2), «Вымпел Коммуникации» (Билайн), «Мегафон» и «Скартел» (Йота).

Следует отметить, что некоторые сотовые операторы делят свои организации на макро-филиалы, в связи с чем большинство запросов **«Теле2» Тамбовской области** передает сотрудникам безопасности в г. Воронеже. Именно по этой причине **«МТС» Тамбовской области** требует, чтобы в запросах по абонентам иных регионов делали пометку **«с проверкой по всем регионам РФ»**, а **«Мегафон» Тамбовской области** может предоставить информацию исключительно по абонентам в пределах своего макро-филиала по следующим регионам:

 Белгородская область;  
 Воронежская область;

 Краснодарский край;  
 Липецкая область;

 Республика Адыгея;  
 Карачаево-Черкесская  
 Республика;  
 Республика Дагестан;  
 Кабардино-Балкарская  
 республика.

 Республика Алания;  
 Чеченская республика;  
 Республика Ингушетия;  
 Тамбовская область;  
 Ростовская область;  
 Ставропольский край;

«Билайн» является единственным сотовым оператором, который не делится на макро-филиалы и может предоставить информацию по своим абонентам со всех регионов России.

**Данные сведения позволяют определить принадлежность абонентского номера к оператору сотовой связи и региону, и в соответствии с полученной информацией правильно организовать направление запроса.**

Примером преступления, раскрытого путем анализа установочных данных владельца абонентского номера, является уголовное дело №11801680009000029 (ОД МОМВД «Знаменский»).

### 1.3 Понятие IMEI

IMEI – уникальный номер сотового аппарата.

Данный номер состоит из 15 последовательных чисел, из которых первые 14 определяют происхождение, модель и серийные номер сотового устройства, а 15-ая – контрольная цифра. В предоставляемых сотовыми операторами детализациях последняя контрольная цифра всегда обозначается как «0». Она не имеет целевого значения, поэтому идентификация сотового аппарата при его изъятии всегда происходит по первым 14 цифрам.

Зная IMEI, посредством множества онлайн-сервисов мы можем определить марку и модель сотового телефона. Одним из самых удобных сервисов является [www.imei.info](http://www.imei.info). Рассмотрим на примере алгоритм определения модели сотового телефона с IMEI 353315071569370:



*подбираем последнюю контрольную цифру методом «тыка» (пока не исчезнет надпись «Invalid IMEI») и жмем кнопку «CHECK».*



## И получаем результат

<b>Model:</b>	<b>iPhone 6S (A1688)</b>
<b>Brand:</b>	<b>APPLE</b>
<b>IMEI:</b>	<b>TAC: 353315 FAC: 07 SNR: 156937 CD: 5</b>

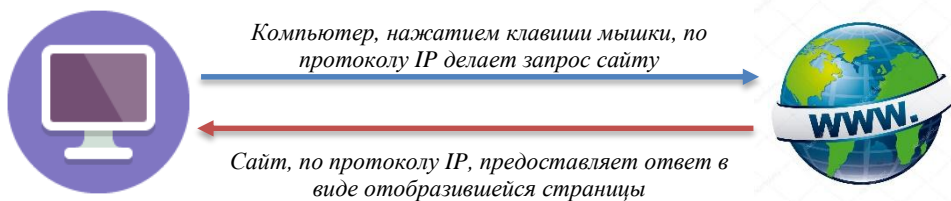
**Информация о конкретной модели и марке телефона облегчит работу при проведении обысков и осмотров, а также позволит определить стоимость телефона. Чем дороже телефон, тем меньше вероятность того, что злоумышленник избавится от него после совершения мошеннических действий, а следовательно будет продолжать его использовать.**

### 1.4 Понятие IP-адреса и средства анонимизации в сети (VPN)

Понять о том, что такое IP-адрес и как он работает первостепенно важно, так как использование сети интернет является краеугольным камнем во многих мошеннических схемах.

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. Процесс соединения компьютера с сайтом в упрощенном виде выглядит следующим образом:




Таким образом, на каждом сайте («ВКонтакте», «Авито», «Юла» и др.) хранится история соединений с его пользователями, а

следовательно и их IP-адреса. При каждом выходе в интернет мошенник оставляет свой «след», по которому его можно вычислить.

Также как и абонентский номер, IP-адрес имеет свой ресурс нумерации, то есть каждому интернет провайдеру выделено определенное количество IP-адресов в конкретном диапазоне.

При помощи интернет ресурса [www.2ip.ru](http://www.2ip.ru) (прямая ссылка: [www.2ip.ru/whois/](http://www.2ip.ru/whois/)), зная IP-адрес, можно легко определить провайдера. Рассмотрим на примере IP-адреса: 178.218.36.0:

IP	178.218.36.0
Хост:	178-218-36-0.pppoe.atexplus.net
Город:	<u>Рыбинск</u> ⚠
Страна:	 <a href="#">Russian Federation</a>
IP диапазон:	178.218.32.0 - 178.218.47.255
CIDR:	178.218.32.0/20
Название провайдера:	<u>ATEXS PLUS Ltd.</u>

*Установлено, что IP-адрес 178.218.36.0 принадлежит провайдеру «Атэкс плюс» в г. Рыбинске (в адрес указанного провайдера и нужно направлять запрос).*

**ВЫВОД:** установив IP-адрес и точное время его использования в сети интернет, сотрудник может узнать адрес нахождения персонального компьютера, с которого работал злоумышленник (адрес квартиры, частного дома или кафе). Примеров уголовных дел, раскрытых при помощи определения IP-адреса, множество: №201607356 (ОД ОП №3 УМВД г. Тамбова), №201607242 (ОД ОП №3 УМВД г. Тамбова), №11801680034000295 (СО ОП №3 УМВД г. Тамбова), №201606986 (СО ОП №3 УМВД г. Тамбова) и другие.

Получение сведений по IP-адресам усложняет использование мошенниками легкодоступных средств анонимизации в сети, которые называются **VPN** (виртуальная частная сеть). Смысл виртуальной частной сети заключается в том, что пользователь интернета, перед тем как выйти на сайт, подключается к серверу третьего лица, как правило локализуемого на территории иного государства. Схематично работа виртуальной частной сети выглядит следующим образом:





По сути запрос на интернет-сайт проходит аналогичным образом, какой был описан ранее, однако в истории соединений сайта остается не реальный IP-адрес пользователя, а IP-адрес использованного им VPN-сервера, который, как показывает практика, в большинстве случаев принадлежит иностранным интернет провайдерам, которым направить запрос в рамках Российского правового поля не представляется возможным.

О том, каким образом можно обойти данную попытку мошенника скрыть себя в сети, мы поговорим после в подразделе «Понятие Cookie-файлов».

### **1.5 Ресурсы, используемые для хранения и перевода похищенных денежных средств**

Основной целью любого мошенничества является хищение материальных ценностей. В случае телефонных и интернет мошенничеств – денежных средств.

Для хранения, использования и вывода похищенных денежных средств злоумышленники используют:

- |                         |                      |
|-------------------------|----------------------|
| ✚ банковские карты;     | ✚ счета абонентских  |
| ✚ расчетные счета;      | номера;              |
| ✚ электронные кошельки; | ✚ наличные переводы. |

Существует множество сервисов наличных переводов – «Колибри», «Вестерн Юнион», «Золотая корона» и др. Работа указанных сервисов заключается в передаче денежных средств на ФИО получателя с указанием контрольной информации – кода или пароля. Таким образом, получить переведенные деньги сможет только лицо, предъявившее удостоверяющий личность документ, а также сообщившее кодовое слово или комбинацию.

С понятием расчетного счета знаком каждый обыватель, однако при расследовании уголовного дела следует обратить внимание на следующее: в большинстве случаев мошенники используют расчетные счета, открытые на подставных лиц, поэтому они не могут лично обратиться в банк с просьбой снять денежные

средства или перевести их на другой счет или банковскую карту – для этого они используют онлайн-ресурсы (ДБО – дистанционное банковское обслуживание) на сайте банка, тем самым оставляя свой след в виде IP-адреса.

Следует иметь в виду, что мошенники, с целью ввести в заблуждение потерпевших и сотрудников полиции, зачастую сообщают ложные сведения о принадлежности карты к банку. Например: «Переведите предоплату на счет банковской карты ВТБ 4276 6100 0000 0000». Не смотря на указание мошенника на принадлежность карты к банку ВТБ, фактически указанная банковская карта выпущена и обслуживается ПАО «Сбербанк». Для того, чтобы верно направить запрос и не терять драгоценное время в ожидании отрицательного ответа, следует проверять банковские карты на принадлежность. Это сделать довольно просто, если вы знаете что такое **БИН**.



**БИН банка** – банковский идентификационный номер. Это первые шесть цифр номера банковской карты. Через множество интернет сервисов по БИН можно узнать принадлежность банковской карты. Самые распространенные из них – [www.binov.net](http://www.binov.net) и

[www.fraudassets.com](http://www.fraudassets.com). Рассмотрим на примере банковских карт №4890 4900 0000 0000 (сайт [www.binov.net](http://www.binov.net)) и №5106 2100 0000 0000 (сайт [www.fraudassets.com](http://www.fraudassets.com)).

BINS	CTYPE	BANK	RANK	TYPE	COUNTRY
489049	VISA	QIWI BANK (JSC)	DEBIT	PREPAID	RUSSIAN FEDERATION

*БИН №489049 принадлежит «Киви Банк», таким образом, все карты, начинающиеся на эти цифры, принадлежат этой организации.*

BIN: 510621  
 Brand: MASTERCARD  
 Bank: YANDEX.MONEY NBCO LLC  
 Type (Credit/Debit): DEBIT  
 Category: WORLD  
 Country: RUSSIAN FEDERATION  
 Country Code: RU

*БИН №510621 принадлежит банку «Яндекс.Деньги», таким образом, все карты, начинающиеся на эти цифры, принадлежат этой организации.*

Электронные кошельки, наиболее популярными представителями которых являются «Киви банк», «Яндекс.Деньги», «ВэбМани» и «Тинькофф – мобильный кошелек», излюбленные ресурсы интернет мошенников, так как для их создания необходим только абонентский номер. Данные организации не имеют представительств, поэтому все операции производят онлайн. Обычный не идентифицированный кошелек имеет мало возможностей – хранение не более 15 000 рублей, оборот не более 40 000 рублей в месяц, запрет на вывод денежных средств в иные платежные сервисы, способен совершать только интернет покупки и онлайн платежи. Полностью же идентифицированный кошелек имеет все возможности банковских карт. Кроме того, на один электронный кошелек можно открыть бесконечное множество виртуальных платежных карт, то есть сервис электронных кошельков номинально выдает пользователю контрольные данные по платежной карте без ее пластикового носителя. Основная информация, которую возможно получить по электронному кошельку (помимо установочных данных владельца и движения денежных средств) – это привязанные к нему абонентские номера и использованные IP-адреса.

Многие мошенники принимают денежные средства на счет абонентских номеров. У каждого сотового оператора есть свои особенности по указанному направлению:

1) расчетные операции по абонентским номерам «Билайн» проводит ЗАО «Национальная сервисная компания». Поэтому данные о движении денежных средств можно запросить как у самого оператора «Билайн», так и у ЗАО «НСК»;

2) расчетные операции по абонентским номерам «МТС» ПАО «Мобильные ТелеСистемы» проводят самостоятельно, поэтому данные о движении денежных средств можно запросить только у самого сотового оператора;

3) расчетные операции по абонентскому номеру «Мегафон» проводит ООО «банк Раунд». Данные о движении денежных средств можно запросить только у данной организации;

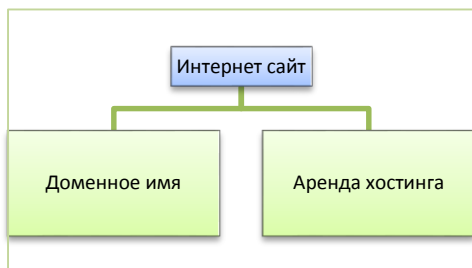
4) у оператора сотовой связи «теле2» нет устоявшегося корреспондента и для проведения расчетных операций он может использовать много сторонних организаций. Информацию о движении денег нужно запрашивать у самого оператора, а после – у корреспондента.

Положительным примером уголовных дел, раскрытых при анализе движения денежных средств и видеоматериалов по местам их снятия, можно указать №11801680013000030 (СО МОМВД «Мордовский»), 11801680001000378 (ОД УМВД г. Тамбова), а также №11801680002000075 (СО ОМВД по г. Котовску).

## 1.6 Понятие интернет сайта. Схема получения информации

**Интернет сайт** - это 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.

Часто встречается такая схема мошеннических действий, при которой злоумышленник создает сайты в виде интернет-магазинов, и похищает денежные средства, «продавая воздух».

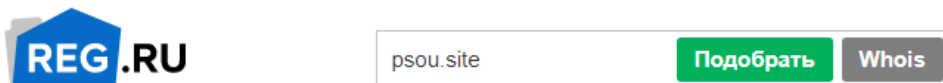


Чтобы получить значимую для уголовного дела информацию следует понимать, что для работоспособности сайта необходимо выполнить два условия: зарегистрировать **доменное имя** и арендовать **хостинг**.

**1) Хостинг.** Как вы храните документы, фотографии, музыку на жестком диске своего компьютера, так и интернет сайт должен иметь свое место для хранения на физическом носителе. Для этого используется специальное оборудование – серверы, подключенные к сети интернет 24 часа в сутки. **Аренда хостинга** – аренда части пространства на данном сервере. Следовательно, чтобы арендовать хостинг необходимо составить соответствующий договор и оплатить предоставляемые услуги. Так как мошенники всегда стараются оставаться в тени, аренду они делают удаленно – через сайты хостинг-арендодателей. **Направив запрос хостинг-арендодателю, возможно получить следующую значимую для расследования дела информацию: данные о лице, осуществившем аренду, а также используемые им банковские карты и счета для оплаты аренды, IP-адреса, электронные почты, абонентские номера и многое другое.**

2) **Доменное имя.** «Доменное имя» - численно-буквенное обозначение, следующее за обозначение всемирной сети («www»). К примеру «vk.com», «youtube.com», «2ip.ru» и др. Доменное имя, также как и хостинг, регистрируется у специальных организаций, и требует регулярной абонентской платы. Направив запрос в организацию-регистратор, возможно получить информацию, аналогичную информации, предоставляемой хостинг-арендодателем.

Организаций-арендодателей хостинга и организаций-регистраторов огромное множество, поэтому для верного направления запроса необходимо правильно получать первоначальные сведения по сайту, или WHOIS-сведения. Это довольно просто - в этом нам поможет интернет ресурс [www.reg.ru](http://www.reg.ru). Рассмотрим на примере сайта-мошенника [www.psou.site](http://www.psou.site):



Заходим на сайт [www.reg.ru](http://www.reg.ru), вводим доменное имя интересующего сайта, нажимаем кнопку «Whois» и получаем нужную информацию:

### Информация о домене

Скачать в PDF

```
Domain Name: PSOU.SITE
Registry Domain ID: D48620238-CNIC
Registrar WHOIS Server: whois.reg.ru
Registrar URL: https://www.reg.ru/
Updated Date: 2018-06-13T21:47:08.0Z
Creation Date: 2017-06-13T10:07:08.0Z
Registry Expiry Date: 2019-06-13T23:59:59.0Z
Registrar: Registrar of Domain Names REG.RU, LLC
Registrar IANA ID: 1606
Domain Status: clientHold https://icann.org/epp#clientHold
Domain Status: autoRenewPeriod https://icann.org/epp#autoRenewPeriod
Registrant Organization: Privacy Protection
Registrant State/Province:
Registrant Country: RU
Name Server: NS1.EXPIRED REG.RU
Name Server: NS2.EXPIRED REG.RU
```

Среди предоставленной информации интерес для расследования уголовного дела представляют фактически следующие две графы:

1) **Строка «Registrar» (или «регистратор»)** – обозначает данные организации, у которой было зарегистрировано доменное имя. В случае с сайтом [www.psou.site](http://www.psou.site) – это ООО «Регистратор доменных имен Рег.Ру». Указанному юридическому лицу следует направлять соответствующий запрос.

2) **Строка «Name Server» (или «DNS сервер»)** - указывает сайт организации, предоставляющей хостинг для сайта. Для рассматриваемого нами сайта это все тот же ООО «Регистратор доменных имен Рег.Ру».

Одним щелчком мышки мы получили нужную информацию – установили, что доменное имя сайта [www.psou.site](http://www.psou.site) было зарегистрировано у организации ООО «Рег.Ру», а также что у данной организации был арендован хостинг.

Кроме того, использованный ресурс [www.reg.ru](http://www.reg.ru), может предоставить сведения WHOIS в виде справки, которую следует приобщить к материалам уголовного дела – для этого необходимо нажать кнопку «Скачать в PDF» (см. фото ранее).

## 1.7 SIP-телефония. Звонки через интернет

Мы часто встречались в своей повседневной жизни с абонентскими номерами, которые начинались на «8-800-...». Эти номера наиболее яркие представителя SIP-телефонии.

SIP-телефония отличается от привычной сотовой связи тем, что она не требует от стороны наличия сотового аппарата или подключения к базовой станции – все звонки поступают на персональный компьютер или смартфон через специальное приложение по протоколу IP, подобно «звонку» на сайт (см. раздел 1.4). Схема связи такого телефонного разговора в упрощенном виде такова:

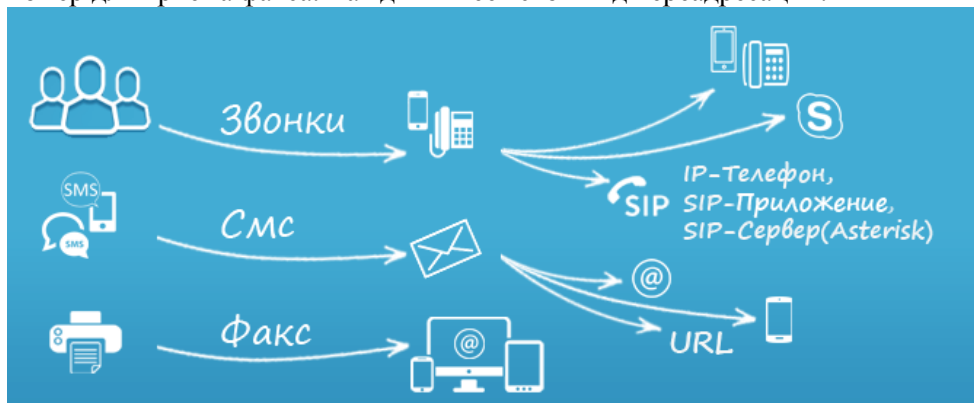


При этом для звонящего каких-либо видимых изменений не происходит – он набирает номер и говорит по телефону, однако для мошенника это больше похоже на входящий вызов в «Skype», «Viber» или «WhatsApp».

Абонентский номер, который использует мошенник при использовании SIP-телефонии, не имеет физического носителя (Sim-карты), он **виртуальный**, при таких обстоятельствах получить информацию в виде привязки к конкретной базовой станции невозможно. Возможно получить лишь сведения об использованных мошенником IP-адресах, которые он использовал для подключения к приложению (сайту) по работе с SIP-провайдером.

**Виртуальный номер** – это основная услуга SIP-провайдера, которая работает через интернет по принципу переадресации звонков. Виртуальные

номера бывают 3 видов: номер для приема звонков, номер для приема SMS, номер для приема факса. Каждый имеет свой вид переадресации:



Отличительными особенностями SIP-телефонии являются:

✚ входящие звонки могут поступать на несколько компьютеров одновременно, при условии, что все они подключены к одному аккаунту (стандартная работа всех Call-центров, когда вам отвечает первый освободившийся специалист);

✚ на один аккаунт можно зарегистрировать бесконечное количество виртуальных номеров, но каждый из них требует оплаты;

✚ в случае, если звонки были переадресованы с виртуального номера на реальный, мы имеем возможность получить сведения об использованных базовых станциях и IMEI последнего;

✚ виртуальные номера могут иметь **любой вид**, как привычный нам 8 (800) 000-00-00, так и 8 (499) 000-00-00, 8 (475) 20-00-00 и др. В редких случаях – даже абонентский номера операторов сотовой связи (МТС, Мегафон и т.д.).

Поэтому если мошенником был использован абонентский номер, внешне похожий на стационарный (с указанием кода любого города), можете быть уверены – это виртуальный номер SIP-провайдера. Ни один мошенник не может быть на столько глуп, чтобы звонить с домашнего телефона.

Таким образом, **от SIP-провайдера можно получить следующую информацию:** установочные данные владельца виртуального номера, информацию об иных номерах, арендованных им, реальный абонентский номер и адрес электронной почты, использованные мошенником IP-адреса, банковские карты и счета, и другую значимую информацию.

Осталось ответить на один вопрос – как понять какому SIP-провайдеру принадлежит тот или иной виртуальный номер? Очень просто, для этого необходимо воспользоваться ресурсом нумерации «Федерального агентства связи», про который мы говорили ранее в **разделе 1.2** ([www.rossvyaz.ru](http://www.rossvyaz.ru)).

## 1.8 Понятие Cookie-файлов как средства деанонимизации мошенника в сети интернет

В разделе 1.4 мы говорили о понятии IP-адреса и наиболее популярном сервисе анонимизации в сети интернет – VPN. В данном разделе будет разъяснено понятие Cookie-файлов, как способ обойти защиту мошенника.

Я думаю многие замечали, что стоит вбить в поисковую строку «Яндекс» или «Google» запрос об определенном типе товара, как браузер начинает выдавать рекламу именно о нем. К примеру, написав «Купить коляску недорого», появляется куча всплывающих окон с рекламой колясок, детского питания, игрушек и прочих вещей по данной тематике. Все дело в том, что **множество интернет сайтов** (но не все) **хранят информацию о своих пользователях**. Сбор и анализ этой информации происходит посредством Cookie-файлов.

**Cookie-файл** – это фрагмент данных, который интернет сайт передает в интернет-браузер (Google Chrome, Mozilla Firefox и др.) своего нового пользователя, чтобы «запомнить» его. При следующем посещении данного сайта, он уже будет «знать» о подключившемся пользователе ряд информации, которая будет расти с каждым последующим посещением:

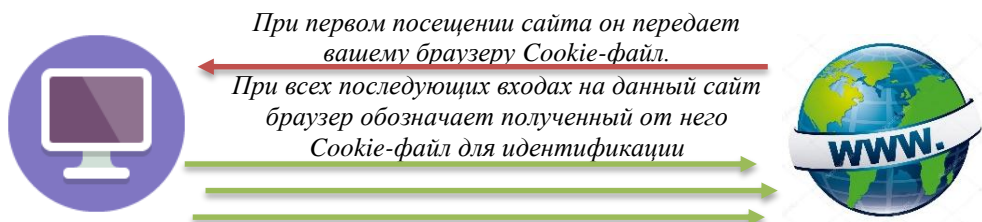
✚ сайт запоминает ваши логины и пароли – именно благодаря Cookie-файлам вам не нужно каждый раз заново вводить пароли в социальных сетях и других сайтах;

✚ сайт запоминает предпочитаемый вами язык;

✚ сайт запоминает последние просматриваемые вами страницы;

✚ **сайт запоминает историю ваших посещений** (данная функция Cookie и имеет для нас ключевое значение).

Схематично Cookie работает следующим образом:





Важной особенностью Cookie-файлов является их неизменность – мошенник сколько угодно раз может менять свой IP-адрес через VPN, проходить регистрацию с разных абонентских номеров, но сайт все равно поймет, что все это время к нему подключается один и тот же пользователь, то есть **используется браузер одного и того же персонального компьютера**.

Каким же образом это может помочь при расследовании уголовного дела? Рассмотрим ответ на данный вопрос на примере мошеннической схемы через сайт «Авито»:

Иванов И.И. регулярно размещает на сайте «Авито» мошеннические объявления о продаже автомобильных запчастей, при этом перед входом на сайт подключается к VPN, чтобы его реальный IP-адрес оставался неизвестным. По одному из таких объявлений ему звонит мужчина из Тамбова и вносит предоплату на счет указанной банковской карты или абонентского номера, тем самым став жертвой мошеннических действий.

Делает запрос на сайт «Авито» о предоставлении информации о лице, разместившем данное мошенническое объявление, необходимо также запросить провести анализ Cookie-файлов мошенника с целью установления **всех объявлений**, которые размещались с браузера данного персонального компьютера, а также информацию **о всех IP-адресах**, использованных для посещения сайта.

Таким образом, имея изначально информацию лишь по одному объявлению мошенника, возможно получить сведения по всем объявлениям, размещенным указанным лицом. Целесообразно провести анализ всех объявлений мошенника с целью определения **реальных объявлений, выложенных с данного персонального компьютера**, с указанием личных IP-адресов и личного абонентского номера. Эти объявления мог разместить сам Иванов И.И. до того, как начал заниматься мошенничеством, или же их мог создать один из членов его семьи, воспользовавшись его компьютером, тем самым раскрыв реальные персональные данные мошенника.



Также давайте не будем забывать о человеческом факторе – возможно при создании одного из мошеннических объявлений Иванов И.И. просто забыл подключиться к VPN.



Примером использования Cookie-файлов для раскрытия преступления можно указать уголовное дело №11801680034000295, возбужденное СО ОП №3 УМВД России по г. Тамбову.


## **2. Сведения, представляющие интерес для расследования уголовного дела**


### **2.1 Сведения, которые необходимо запрашивать у сотовых операторов**


С информацией о запрашиваемых сведениях можно ознакомиться в разделах 1.1 – 1.5:

-  паспортные данные владельца абонентского номера;
-  детализация звонков за последние три месяца – эти сведения позволяют определить, сколько у мошенника сотовых аппаратов (IMEI), как часто он меняет абонентские номера, а также избавляется ли он от Sim-карты после совершения мошеннических действий или же использует повторно;

-  использованные для связи IMEI за последние три месяца;
-  использованные для связи базовые станции за последние три месяца с указанием следующих технических характеристик: количество секторов (антенных блоков в месте установки), азимут направленности использованных антенных блоков и угол охватываемой ими территории;

-  информацию о входящих и исходящих платежах по лицевому счету абонентского номера;


-  информацию об IP-адресах, использованных для входа в личный кабинет сотового оператора по управлению данным номером. Так как в большинстве случаев мошенник использует абонентские номера, зарегистрированный на подставных лиц, и все операции по управлению абонентским номером проводит через личный кабинет, тем самым оставляя «след» в виде своего IP-адреса;


-  копию регистрационной формы – документ, который заполняет продавец Sim-карты при ее регистрации. Помимо установочных данных в нем мы узнаем данные о адресе торговой точки, где она была реализована, а также данные продавца. К этому лицу у следствия также должны возникнуть обоснованные вопросы.


### **2.2 Сведения, которые необходимо запрашивать по банковским картам и расчетным счетам**


С информацией о запрашиваемых сведениях можно ознакомиться в разделах 1.4 – 1.5.


### По банковской карте:

 информацию о паспортных данных владельца банковской карты;


 информацию о движении денежных средств по банковской карте и местах их обналичивания за последние полгода с указанием точного времени проведения приходных и расходных операций, номера и коды транзакций и др. Проанализировав полученную информацию за последние полгода, возможно определить наиболее часто используемые банкоматы, которые, как показывает практика, находятся рядом с домом мошенника или местом частого посещения (работа, торговый центр, адрес родственников и т.д.), информацию о регулярно оплачиваемых абонентских номерах (личный номер, номер родственников или друзей); а также о торговых точках или интернет магазинах, на которых совершались покупки. Каждый интернет-магазин предоставит информацию об адресе мошенника, на который почтовым переводом был отправлен приобретенный товар.

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

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


 информацию об IP-адресах, использованных для входа в онлайн-сервис по управлению данной банковской картой.


По расчетному счету необходимо запрашивать аналогичную информацию, а также:







 информацию о банковских картах, открытых по данному расчетному счету.

## **2.3. Сведения, которые необходимо запрашивать по электронным кошелькам (Qiwi, Яндекс.Деньги и др.)**

С информацией о запрашиваемых сведениях можно ознакомиться в разделах 1.4 и 1.5:

 информацию о паспортных данных владельца электронного кошелька;




 информацию о способе и месте идентификации электронного кошелька;

-  информацию об абонентском номере, с использованием которого был создан электронный кошелек;
-  информацию об абонентских номерах, привязанных к электронному кошельку;
-  информацию о виртуальных банковских картах, которые были выпущены по данному электронному кошельку;
-  информацию о пластиковых картах, выпущенных по данному кошельку, способ их получения (адрес почтового отправления);
-  информацию о входящих и исходящих платежах по электронному кошельку с момента его регистрации;
-  информацию об IP-адресах, использованных для совершения денежных транзакций, а также администрирования электронного кошелька.


## **2.4 Сведения, которые необходимо запрашивать по сайтам объявлений (Авито, Юла и др.)**

С информацией о запрашиваемых сведениях можно ознакомиться в разделах 1.4 и 1.8:

### Если мошенник выступает как продавец:


-  информацию о лице, разместившем объявление о продаже (наименование товара) с абонентского номера (номер мошенника):
  - установочные данные;
  - использованные им для регистрации абонентские номера и электронные почты;
  - использованные для создания и администрирования объявлений IP-адреса.
-  аналогичную информацию о иных объявлениях данного лица, созданных с использованием того же абонентского номера или электронной почты;
-  аналогичную информацию о иных объявлениях данного лица, установленных при анализе Cookie-файлов.

### Если мошенник выступает как покупатель:


-  информацию об IP-адресах пользователей сайта, просматривавших объявление потерпевшего (номер объявления).

## 2.5. Сведения, которые необходимо запрашивать по социальным сетям.

С информацией о запрашиваемых сведениях можно ознакомиться в разделах 1.4 и 1.8:


 информацию о пользователе страницы социальной сети (ссылка на страницу, например <https://vk.com/id410077130>):


- установочные данные,
- использованные им для регистрации абонентские номера и электронные почты;
- IP-адреса использованные для создания и доступа к странице за последние два месяца;


 аналогичную информацию по иным страницам социальной сети «ВКонтакте» данного пользователя, установленных при анализе Cookie-файлов (данный пункт не запрашивается в случае взлома страницы потерпевшего или страниц его друзей).


## 2.6. Сведения, которые необходимо запрашивать по доменному имени сайта


С информацией о запрашиваемых сведениях можно ознакомиться в разделах 1.4, 1.6 и 1.8:


 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 регистрации доменного имени;


 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.


## **2.7 Сведения, которые необходимо запрашивать по арендуемому хостингу**


С информацией о запрашиваемых сведениях можно ознакомиться в разделах 1.4, 1.6 и 1.8:


 информацию о паспортных данных арендатора хостинга;


 информацию об использованных для аренды абонентских номерах и электронных почтах;

 информацию о том, каким образом была произведена регистрация пользователя;

 информацию об IP-адресах, использованных для аренды хостинга;


 информацию об IP-адресах, использованных для входа в личный кабинет или панель управления для администрирования хостинга;

 информацию об оплате услуг аренды хостинга, с указанием полных реквизитов плательщика;

 аналогичную информацию по иным хостингам, арендуемым данным пользователем, установленным при анализе Cookie-файлов.


## **2.8 Сведения, которые необходимо запрашивать у Интернет-провайдера**




С информацией о запрашиваемых сведениях можно ознакомиться в разделах 1.4:

 информацию о пользователе и адресе использованного оборудования, которому был выдан интересующий нас IP-адрес в интересующий нас промежуток времени.

## **2.9. Сведения, которые необходимо запрашивать по электронной почте**










С информацией о запрашиваемых сведениях можно ознакомиться в разделах 1.4:

 информацию о паспортных данных владельца электронной почты;

-  информацию об использованных для регистрации абонентских номерах;
-  информацию об IP-адресах, использованных для доступа к электронной почте за максимально известный период;
-  аналогичную информацию по иным электронным почтам, зарегистрированным данным пользователем, установленным при анализе Cookie-файлов.

## **2.10 Сведения, которые необходимо запрашивать у провайдера SIP- телефонии.**

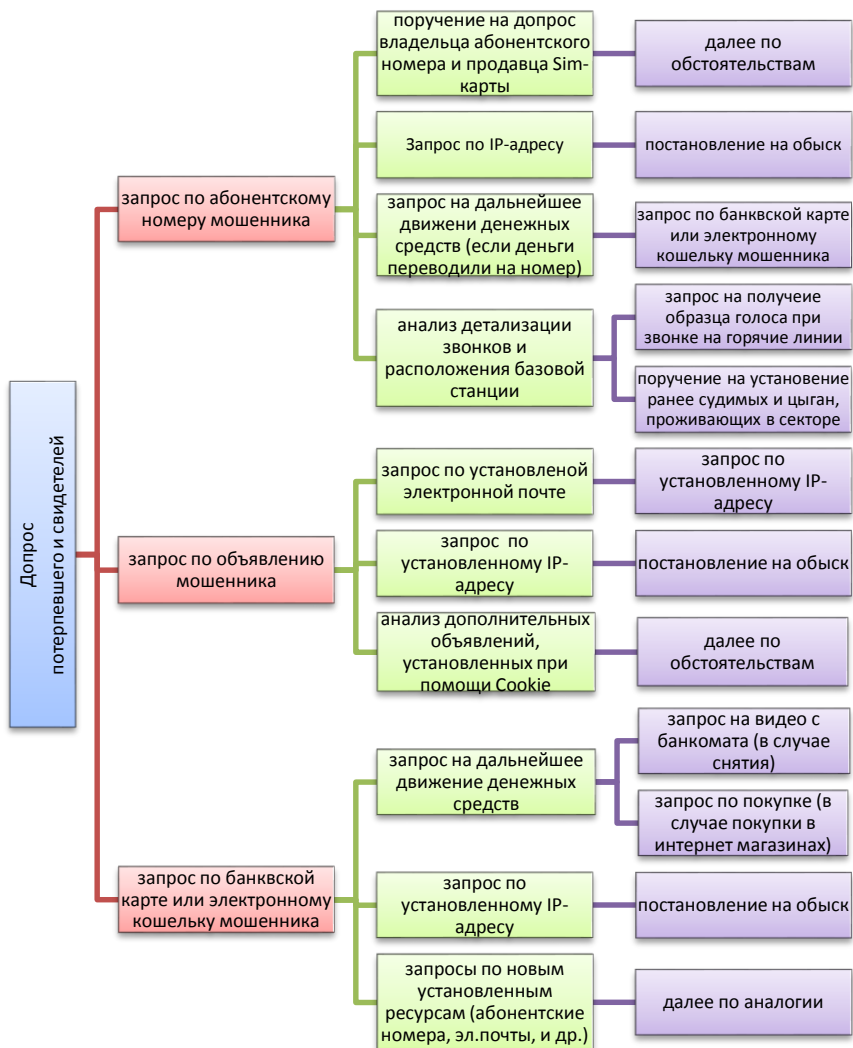
С информацией о запрашиваемых сведениях можно ознакомиться в разделах 1.4, 1.6-1.8:

-  информацию о паспортных данных владельца абонентского номера;
-  информацию об использованных для регистрации абонентских номерах, электронных почтах;
-  информацию о том, каким образом была произведена регистрация пользователя;
-  информацию об IP-адресах, использованных для регистрации абонентского номера;
-  информацию об IP-адресах, использованных для входа в личный кабинет, панель управления по администрированию данным абонентским номером;
-  информацию об IP-адресах, использованных для осуществления звонков;
-  информацию об абонентских номерах, на которые шла переадресация звонков;
-  статистика звонков за интересующий период;
-  информацию об оплате услуг связи, с указанием полных реквизитов плательщика;

### 3. Схемы расследования наиболее частых телефонных и интернет мошенничеств.

#### 3.1. Схема 1. Мошенничества через сайты объявлений. Мошенник-продавец

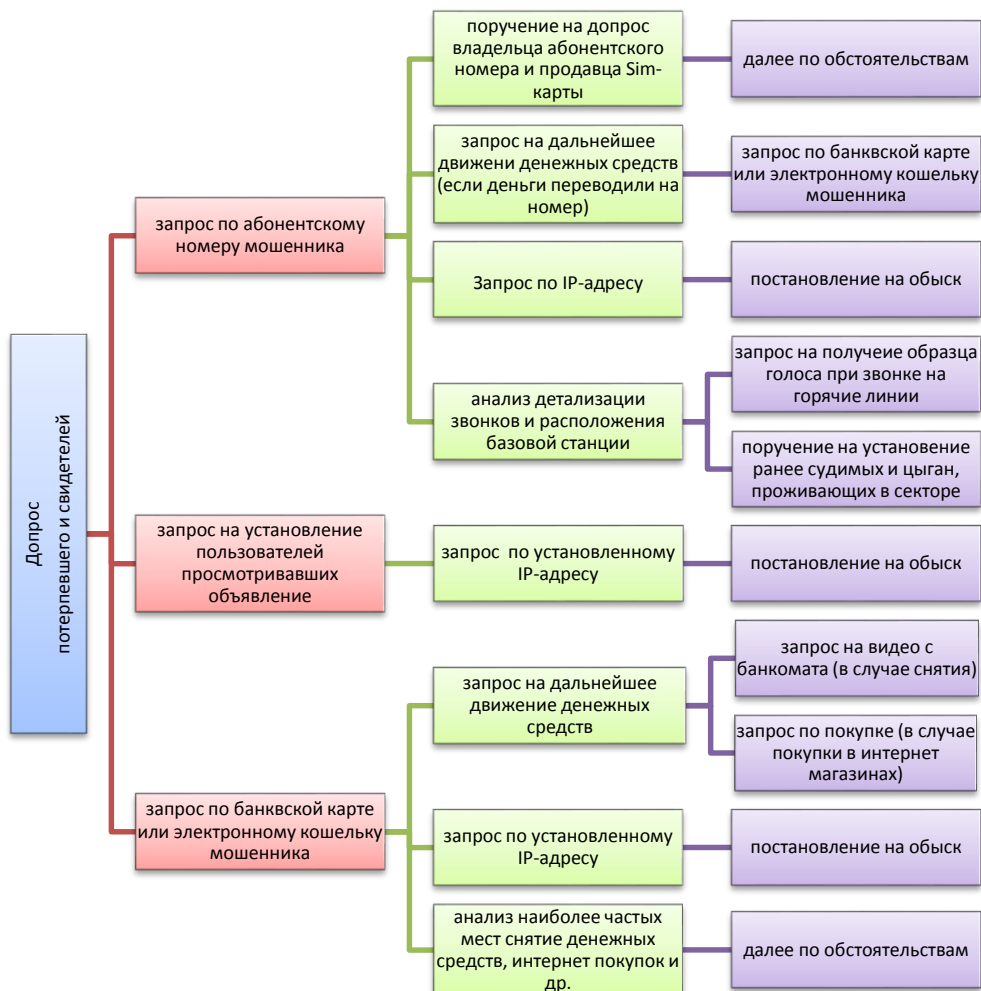
Мошенник размещает на сайтах объявлений (Авито, Юла, Циан и др.) информацию о продаже какого-либо товара, сдаче в аренду жилых помещений или же оказании тех или иных услуг, за которые в последующем получает предоплату, тем самым похищая деньги.





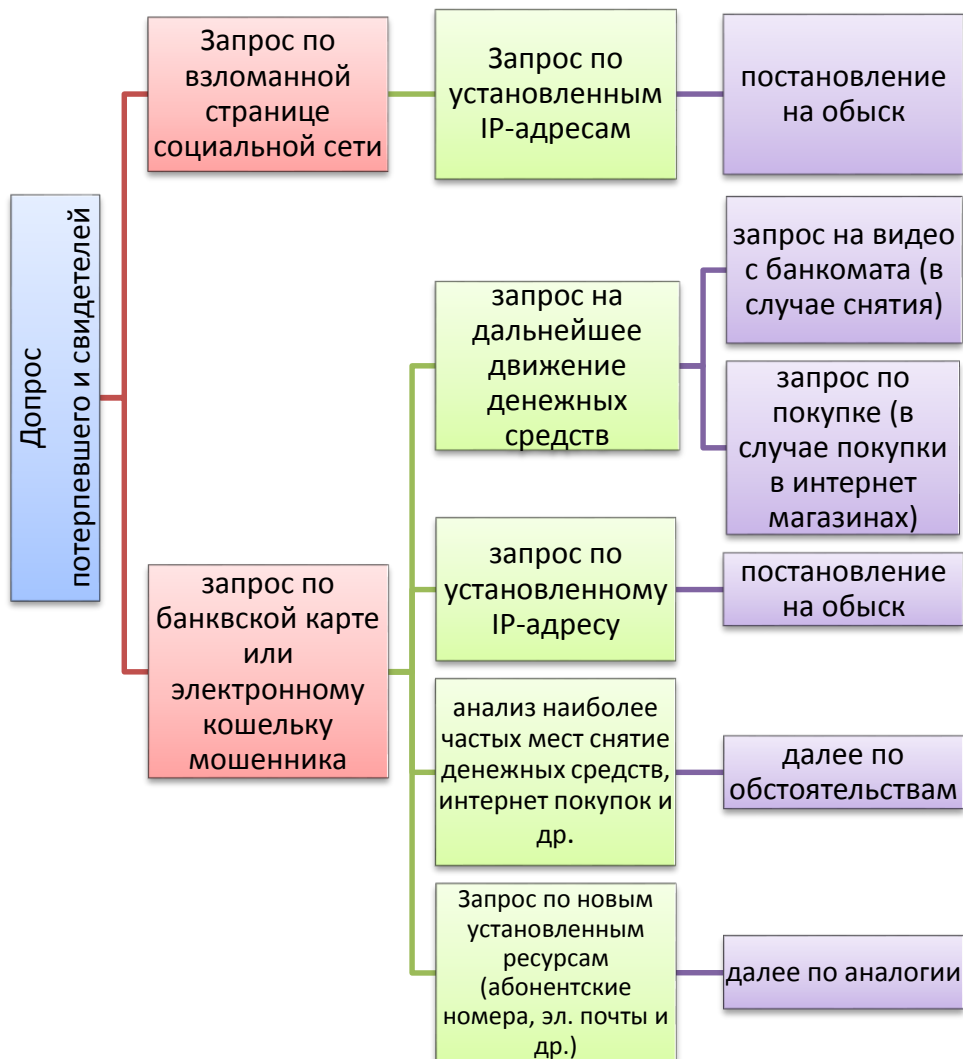
### 3.2. Схема 2. Мошенничества через сайты объявлений. Мошенник-покупатель.

Мошенник звонит по объявлению потерпевшего, размещенному на сайте (Авито, Юла, Циан и др.) и говорит, что желает приобрести его товар и готов внести задаток, для чего просит продиктовать контрольные данные по банковской карте и поступивший код. Получив данные сведения осуществляют перевод через онлайн сервисы или совершая покупку. Или же мошенник просит подойти к банкомату и выполнить ряд комбинаций, подключая мобильный банк, и в последующем похищая денежные средства.



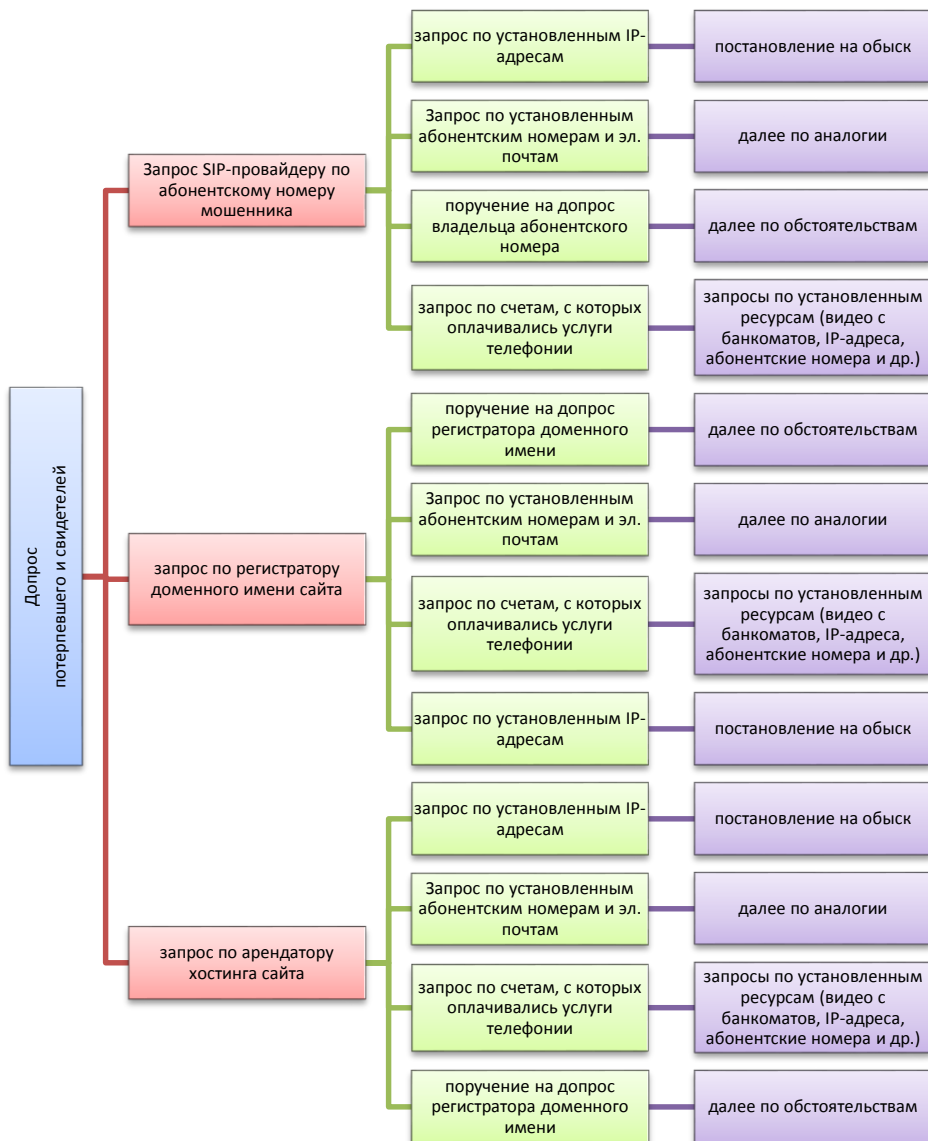
### 3.3. Схема 3. Мошенничества со взломом страниц социальных сетей

Мошенник покупает в сети интернет взлом страницы социальной сети (Вконтакте, Одноклассники, Друг Вокруг и др.) или осуществляет его самостоятельно. В последующем пишет всем друзьям из списка сообщения мошеннического характера с просьбой занять денежные средства под различными предложениями (заболел родственник, не хватает на срочную покупку и т.д.).



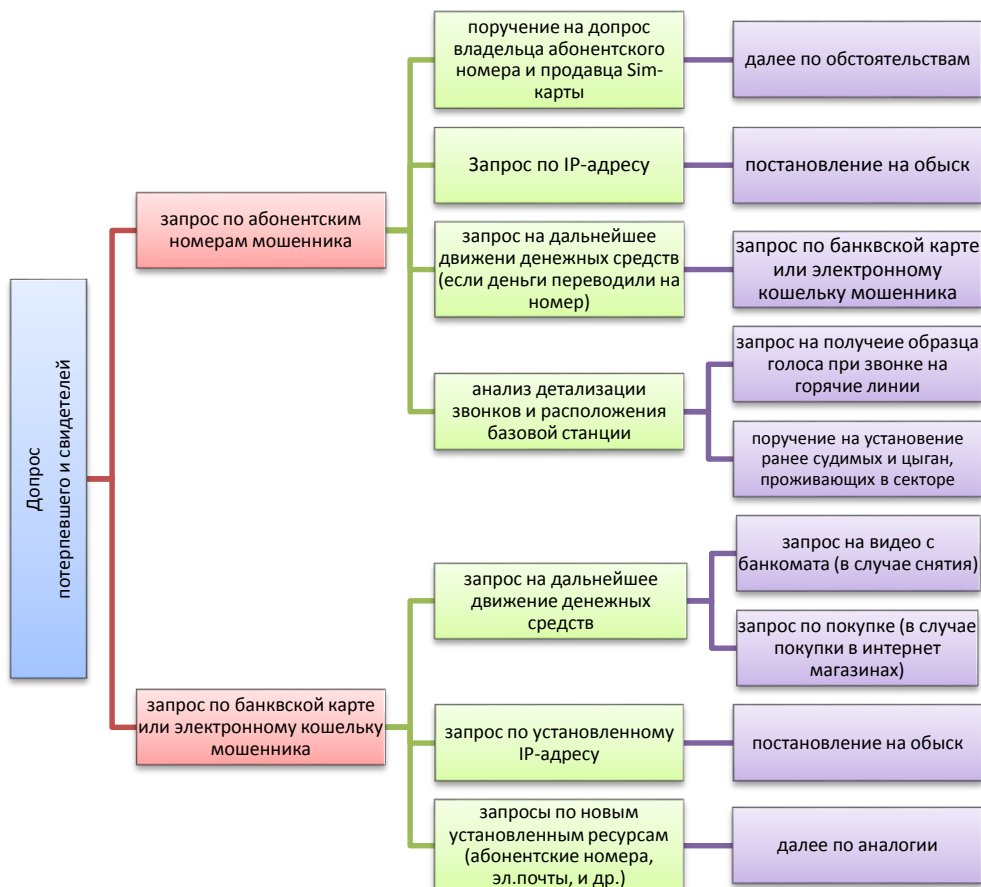
### 3.4 Схема 4. Мошенничества, совершенное с использованием интернет сайтов (Интернет магазинов)

Мошенник создает (или покупает) интернет сайт по продаже товара различной тематики. Регистрирует несколько виртуальных номеров (8-800-..., 8-495-... и др.) у SIP-провайдера и указывает их на сайте в качестве контактов. В последующем принимает покупателей, получая от них денежные средства за покупку товара с сайта.



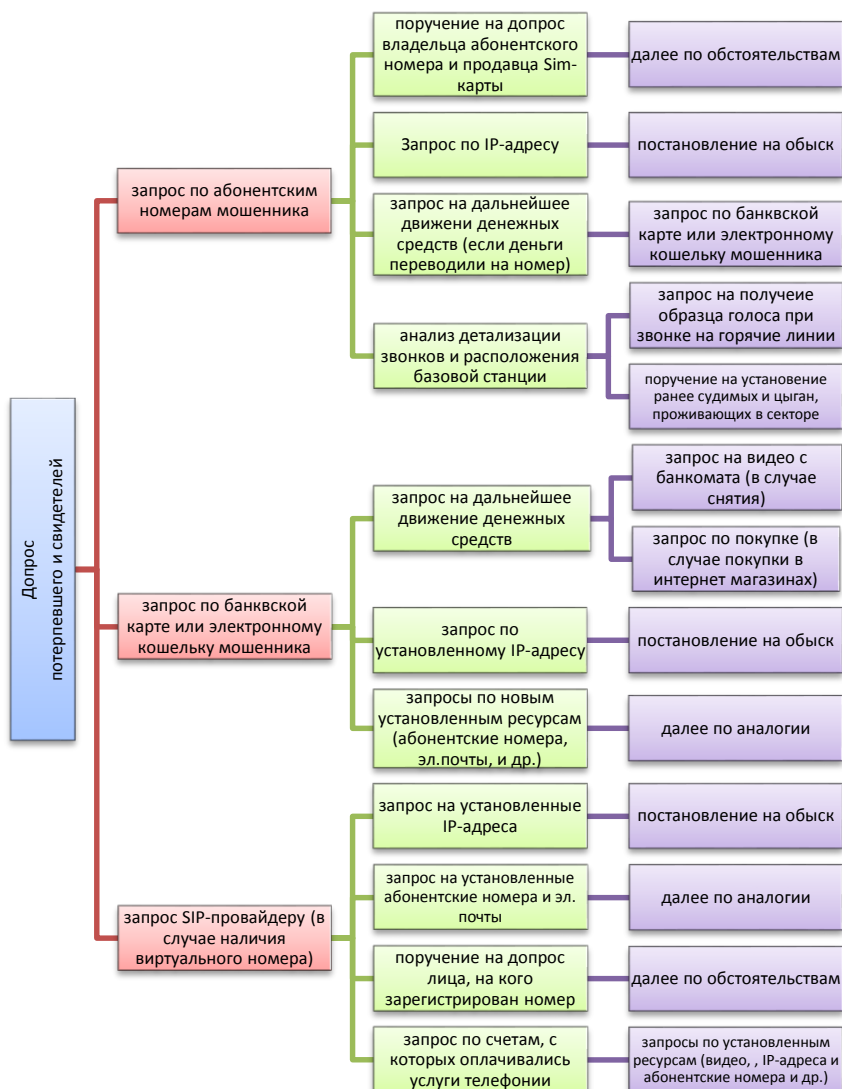
### 3.5 Схема 5. Мошенничество, совершенное под предлогом заказа банкета (или связь с курьером).

Мошенник звонит в организацию и говорит, что желает воспользоваться ее услугами по заказу банкета, заказу крупной партии товара или прочих услуг. Далее он сообщает адрес, где бы он хотел встретиться в представителем компании и спрашивает его телефон. В последующем он связывается с представителем и просит последнего по пути полонить счет абонентского номера (или банковской карты) на неопределенную сумму, которую он отдаст при встрече.



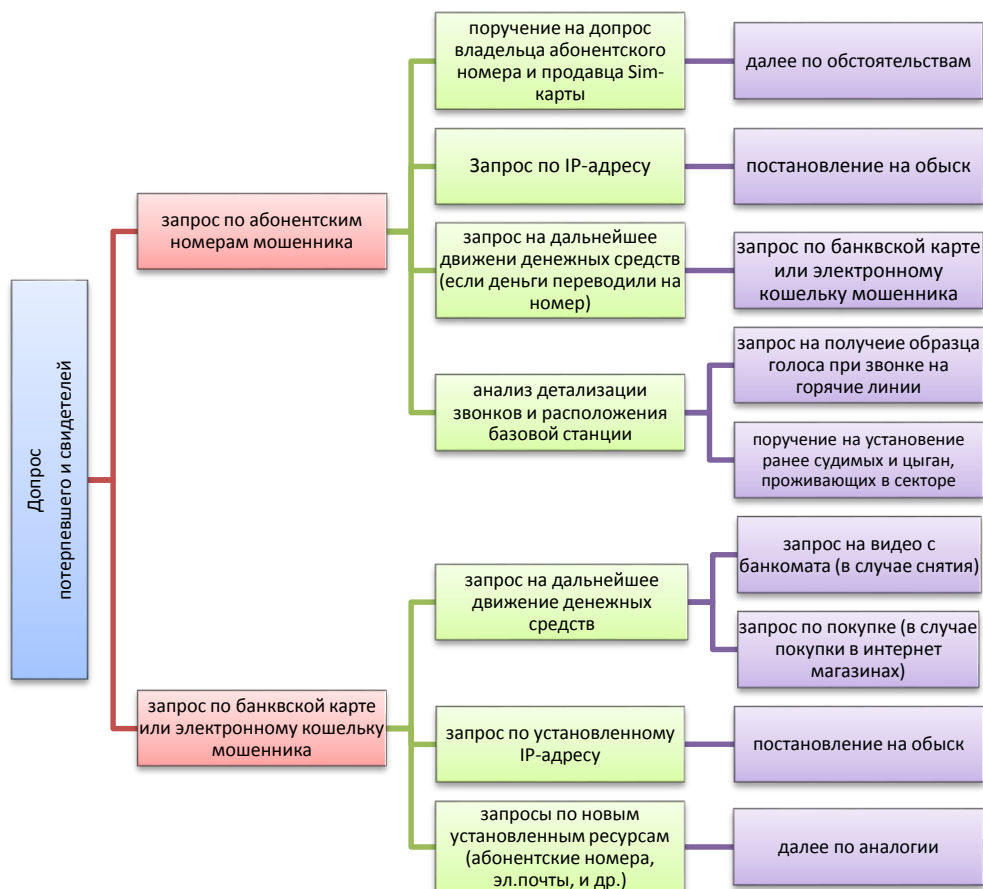
### 3.6 Схема 6. Мошенничество, совершенное под предлогом разблокировки банковской карты или предотвращения списания денежных средств.

Мошенник осуществляет рассылку SMS-сообщений с текстом о списании денежных средств или блокировке банковской карты. В данном сообщении указывает свой другой абонентский номер (иногда виртуальный 8-800-..., 8-495-... и др.), который может проинформировать о произошедшем. Потерпевший звонит по данному номеру, после чего мошенник либо просит сообщить контрольные данные банковской карты, либо просит подойти к банкомату (аналогично схеме 2).



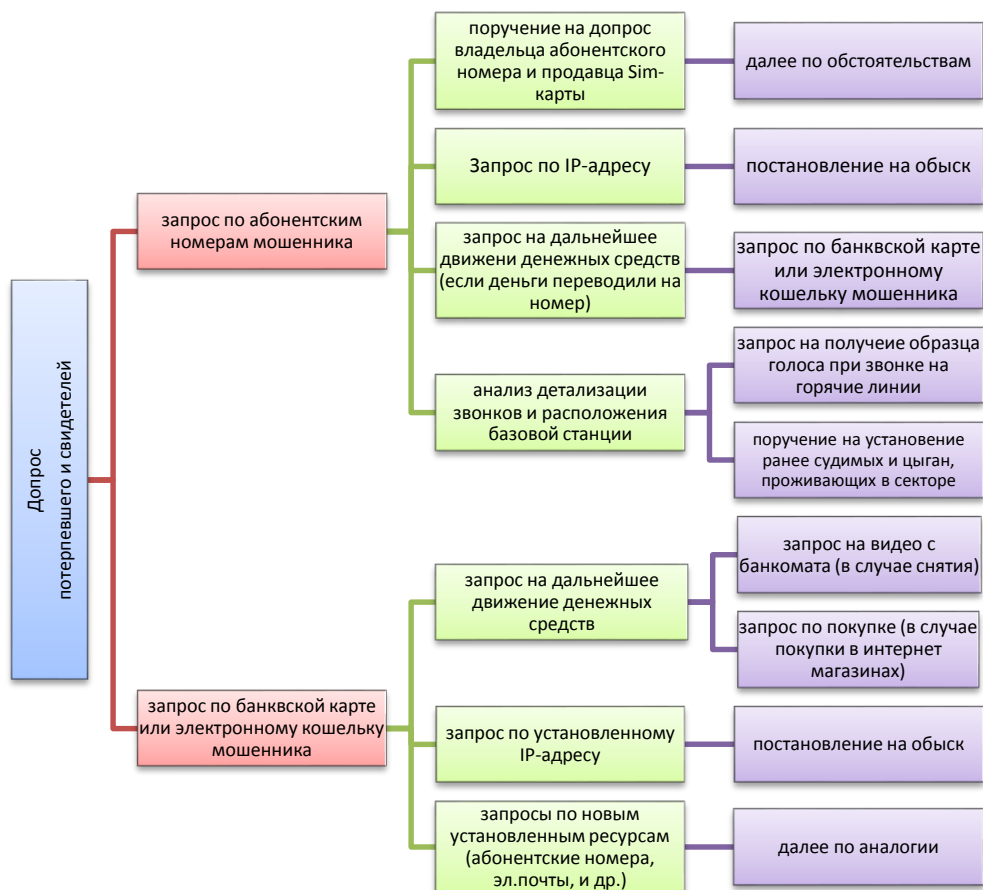
### 3.7 Схема 7. Мошенничество, совершенное под предлогом помощи родственнику, попавшему в беду

На стационарный или абонентский номер потерпевшего звонит мошенник, который обращается под видом родственника (привет мама, привет бабушка и т.д.). Сообщает, что попал в ДТП и сбил человека, с кем-то подрался и т.д., а после передает трубку сотруднику полиции, который за отдельную плату предлагает решить вопрос об отказе в возбуждении уголовного дела.



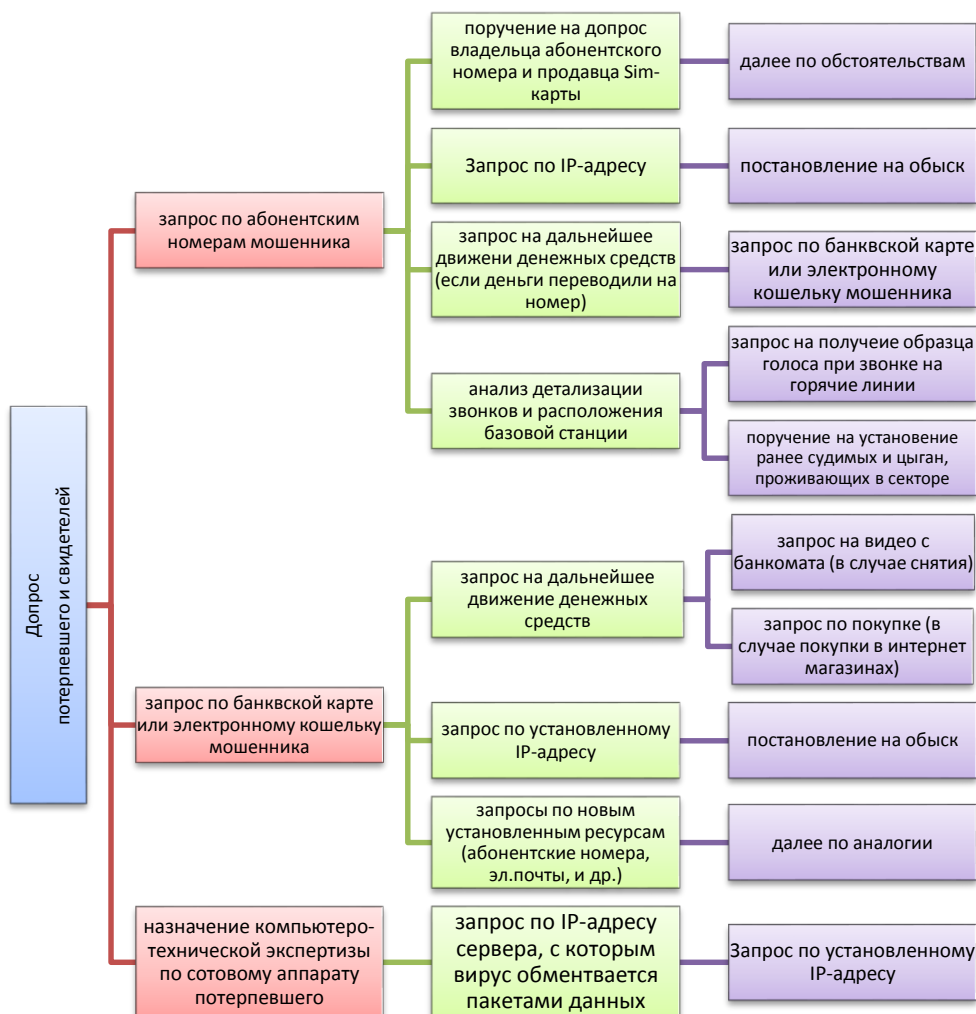
### 3.8 Схема 8. Мошенничество, совершенное под предлогом компенсации за ранее приобретенные БАДы

На стационарный или абонентский номер потерпевшего звонит мошенник, который, представляется сотрудником прокуратуры или правоохранительных органов. Он сообщает, что в настоящий момент задержана группа мошенников, продававших некачественный БАДы, и что потерпевшему положена компенсация. Однако для ее получения необходимо оплатить государственную пошлину или налоговый сбор.



### 3.9 Схема 9. Мошенничество, совершенное с использованием вредоносных программ на ОС «Android»

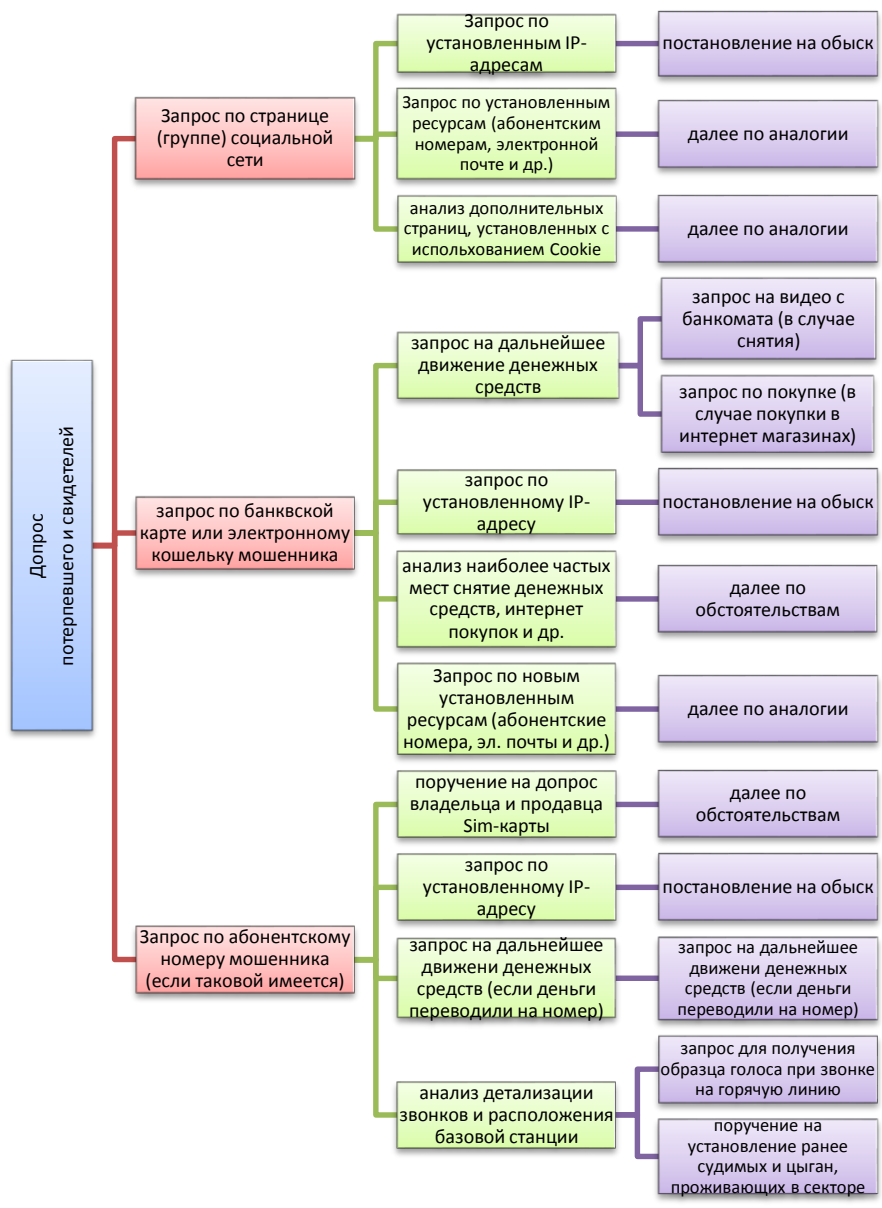
Потерпевшему на сотовый телефон с операционной системой «Android» с неизвестного номера приходят SMS-сообщения с текстом: «Здравствуйте, я по Вашему объявлению. Не интересует обмен с доплатой? Ссылка: [www.avito.ru/FriZkksk](http://www.avito.ru/FriZkksk)», или SMS-сообщение с текстом: «Смотри как мы здорово получились на этой фотографии. Ссылка [www.bit.ly/ZreizE1eaAa](http://www.bit.ly/ZreizE1eaAa)». Потерпевший проходит по данной ссылке, в результате чего загружает на свой телефон вирус (чаще всего используются вирусы под названием «Triada» и «Marcher»), предоставляющий злоумышленнику доступ к SMS-командам. В дальнейшем мошенник похищает деньги, путем направления сообщений на номер «900».





3.10    **Схема 10. Мошенничество, совершенное с использованием социальных сетей (интернет магазин «ВКонтакте»)**

Мошенник создает страницу или группу в социальной сети, позиционирующую себя как интернет-магазин. В последующем принимает покупателей, получая от них денежные средства за покупку товара с сайта



## Заключение

Расследование мошенничеств, совершенных с использованием средств сотовой связи и сети интернет, требует углубленного анализа поступающей информации, индивидуального и творческого подхода к каждому факту совершенного преступления, а также пусть не глубоких, но специфических познаний, расширение объема которых будет приходиться с опытом.

Целесообразно организовать работу по данному направлению путем закрепления сотрудников уголовного розыска, дознания и следствия, по **линейному принципу работы**, обособленно в каждом отделе полиции.

В дополнении хотелось бы напомнить, что мы живем в 21 веке, и помимо традиционных почтовых отправок имеем в своем распоряжении такие вещи как электронная почта и факс. Множество организаций понимают, как важно максимально оперативно получить информацию по преступлениям данного характера, поэтому соглашаются на получение запросов и предоставления ответов посредством электронного документооборота или факса.

**Информацию об уже имеющихся договоренностях с различными организациями по взаимодействию путем электронного документооборота возможно получить в Управлении уголовного розыска УМВД России по Тамбовской области.**

Общеизвестно, что телефонные и интернет мошенничества часто носят межрегиональный характер, поэтому для достижения положительных результатов необходимо поддерживать взаимодействие и осуществлять обмен информацией с представителями правоохранительных органов иных субъектов Российской Федерации.

По всем вопросам, возникшим при ознакомлении с настоящими методическими рекомендациями, а также по вопросам организации работы по раскрытию и расследованию мошенничеств необходимо обращаться к:

**1) *Старшему оперуполномоченному УУР УМВД России по Тамбовской области капитану полиции Козодаеву Андрею Павловичу (8-920-478-88-55, 8-4752-799-666, внутренний – 46-66).***

**2) *Оперуполномоченному по особо важным делам УУР УМВД России по Тамбовской области капитану полиции Меринову Игорю Владимировичу (8-902-726-58-60, 8-4752-799-590, внутренний – 45-90).***