

МВД России

Всероссийский институт повышения квалификации
сотрудников МВД России

**ОСОБЕННОСТИ РАСКРЫТИЯ ПРЕСТУПЛЕНИЙ,
СОВЕРШАЕМЫХ В СОВРЕМЕННОМ
ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ
С ИСПОЛЬЗОВАНИЕМ СЕТИ ИНТЕРНЕТ**

Научно-практическое пособие

*Под общей редакцией начальника БСТМ МВД России
генерал-лейтенанта М. Ю. Литвинова*

Домодедово
ВИПК МВД России
2026

ББК 67.408.135

О 75

Авторский коллектив:

В. И. Алескеров, кандидат юридических наук, доцент; **О. Н. Колокольчикова**; **Е. В. Маркелова**; **В. В. Баранов**, кандидат юридических наук; **А. В. Кононенко**; **А. О. Косцов**.

Рецензенты:

И. Ф. Амельчаков – начальник Санкт-Петербургского университета МВД России генерал-лейтенант полиции;

А. В. Александрович – заместитель начальника БСТМ УМВД России по Еврейской автономной области полковник полиции;

С. В. Катков – профессор кафедры оперативно-розыскной деятельности и специальной техники Волгоградской академии МВД России доктор юридических наук, доцент полковник полиции в отставке;

Р. В. Кириллов – начальник БСТМ ГУ МВД России по Калининградской области полковник полиции.

О 75 Особенности раскрытия преступлений, совершаемых в современном информационном пространстве с использованием сети Интернет : научно-практическое пособие / В. И. Алескеров, О. Н. Колокольчикова, Е. В. Маркелова [и др.]; под общ. ред. М. Ю. Литвинова. – Домодедово : ВИПК МВД России, 2026. – 162 с.

В научно-практическом пособии рассматриваются основные теоретические, правовые и организационные вопросы деятельности сотрудников оперативных подразделений и следователей органов внутренних дел Российской Федерации, способствующие своевременному раскрытию преступлений, совершаемых в современном информационном пространстве с использованием сети Интернет.

Даны общие понятия, необходимые для своевременного раскрытия и расследования преступлений данной направленности, объединенные в глоссарий.

В издании представлены: алгоритм действий, осуществляемых сотрудниками дежурной части и следственно-оперативной группы в случаях поступления оперативно значимой информации о подготавливаемом, совершаемом или уже совершенном преступлении в современном информационном пространстве с использованием сети Интернет; алгоритмы получения информации, представляющей оперативный интерес; актуальные вопросы оперативно-служебной деятельности сотрудников оперативных подразделений и следственных органов внутренних дел Российской Федерации, направленной на своевременное выявление, предупреждение, пресечение и раскрытие преступлений, совершаемых в современном информационном пространстве с использованием сети Интернет; отмечена роль сотрудников уголовного розыска, Управления по борьбе с противоправным использованием информационно-коммуникационных технологий и подразделений специальных технических мероприятий органов внутренних дел Российской Федерации в раскрытии подобных преступлений.

Пособие предназначено для руководителей и сотрудников оперативных подразделений органов внутренних дел Российской Федерации, а также адъюнктов, профессорско-преподавательского состава высших учебных заведений юридического профиля системы МВД России.

ББК 67.408.135

© ВИПК МВД России, 2026

Оглавление

ГЛОССАРИЙ.....	5
ВВЕДЕНИЕ	10
ГЛАВА 1.	
АНАЛИЗ СОСТОЯНИЯ ПРЕСТУПНОСТИ В РОССИИ ЗА 2023–2024 ГГ.	
ОБЩИЕ ПОНЯТИЯ	
СОВРЕМЕННОГО ИНФОРМАЦИОННОГО ПРОСТРАНСТВА	
И СВЕДЕНИЯ О ГЛОБАЛЬНОЙ СЕТИ ИНТЕРНЕТ	15
1.1. Сотовая связь и базовые станции	23
1.2. Абонентский номер	24
1.3. IMEI	25
1.4. IP-адрес и средство анонимизации сети (VPN).....	26
1.5. Ресурсы, используемые для хранения и перевода похищенных денежных средств.....	28
1.6. Интернет-сайт. Схема получения информации.....	32
1.7. IP-телефония. Звонки в современном информационном пространстве с использованием сети Интернет.....	34
1.8. Cookie-файлы как средства деанонимизации мошенника в современном информационном пространстве с использованием сети Интернет	36
1.9. Даркнет (DarkNet) как один из элементов сети Интернет	37
ГЛАВА 2.	
АЛГОРИТМ ДЕЙСТВИЙ СОТРУДНИКОВ	
СЛЕДСТВЕННО-ОПЕРАТИВНОЙ ГРУППЫ И ДЕЖУРНЫХ ЧАСТЕЙ	
ПРИ ПОСТУПЛЕНИИ СООБЩЕНИЯ О ПРЕСТУПЛЕНИИ,	
СОВЕРШЕННОМ В СОВРЕМЕННОМ ИНФОРМАЦИОННОМ	
ПРОСТРАНСТВЕ С ИСПОЛЬЗОВАНИЕМ СЕТИ ИНТЕРНЕТ.....	45
2.1. Действия сотрудников дежурных частей при получении заявления (сообщения) о преступлении, совершенном в современном информационном пространстве с использованием сети Интернет.....	45
2.2. Действия следователей (дознавателей) в процессе расследования уголовных дел до полного выяснения всех обстоятельств и установления лиц, причастных к совершению преступлений в современном информационном пространстве с использованием сети Интернет.....	47
2.3. Действия сотрудников оперативных подразделений при получении информации о преступлении, совершенном в современном информационном пространстве с использованием сети Интернет.....	66

2.4. Действия сотрудников экспертно-криминалистического подразделения в процессе производства необходимых экспертиз с целью установления подозреваемых лиц, причастных к подготавливаемым или уже совершенным преступлениям в современном информационном пространстве с использованием сети Интернет.....	71
2.5. Алгоритм контроля за принятием процессуального решения по сообщениям о преступлениях (происшествиях), совершенных в современном информационном пространстве с использованием сети Интернет.....	72
2.6. Взаимодействие оперативных сотрудников и следователей при раскрытии и расследовании преступлений, совершенных в современном информационном пространстве с использованием сети Интернет.....	73
ГЛАВА 3. ОСОБЕННОСТИ ПОЛУЧЕНИЯ ОПЕРАТИВНО ЗНАЧИМОЙ ИНФОРМАЦИИ СОТРУДНИКАМИ ОПЕРАТИВНЫХ ПОДРАЗДЕЛЕНИЙ И СЛЕДСТВЕННЫХ ОРГАНОВ В ЦЕЛЯХ РАСКРЫТИЯ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ В СОВРЕМЕННОМ ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ С ИСПОЛЬЗОВАНИЕМ СЕТИ ИНТЕРНЕТ.....	81
3.1. Алгоритм действий оперативных сотрудников и следователей, направленных на получение необходимой информации у сторонних компаний, организаций и учреждений.....	81
3.2. Схемы расследования наиболее распространённых преступлений, совершаемых в современном информационном пространстве с использованием сети Интернет.....	85
ГЛАВА 4. РОЛЬ СОТРУДНИКОВ ОПЕРАТИВНЫХ ПОДРАЗДЕЛЕНИЙ ОРГАНОВ ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ В РАСКРЫТИИ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ В СОВРЕМЕННОМ ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ С ИСПОЛЬЗОВАНИЕМ СЕТИ ИНТЕРНЕТ	122
4.1. Исторический аспект оперативно-служебной деятельности Московского уголовного розыска ГУ МВД России по г. Москве	123
4.2. Анализ организации оперативно-служебной деятельности УУР и УБК ГУ МВД России по г. Москве при раскрытии преступлений, совершенных в современном информационном пространстве с использованием сети Интернет.....	126
ЗАКЛЮЧЕНИЕ	147
ЛИТЕРАТУРА	156

Глоссарий

Автоматизированное рабочее место клиента Сбербанка России (АРМ КБР) – программа, необходимая любому банку, действующему на территории Российской Федерации, для предоставления финансовой отчетности в Банк России за определенный период времени.

Анонимизация – совокупность действий, направленных на сокрытие личности пользователя путем маскировки или подмены характеристик пользователя и его устройств.

Анонимизированная личность – замаскированная виртуальная сущность, используемая для создания анонимности.

Банк-эквайер – уполномоченный банк (член платежной системы), осуществляющий первичную обработку транзакций и берущий на себя обязательства в пределах всего спектра операций с банковскими картами.

Банк-эмитент – кредитная организация, участник платежной системы, осуществляет выпуск и обслуживание банковских карт. Выступает гарантом выполнения финансовых обязательств, возникающих в ходе использования карт держателями.

Банковские троянцы (Trojan-Banker) – вредоносные программы, предназначенные для кражи учетных данных систем интернет-банкинга, систем электронных платежей, кредитных или дебетовых карт.

Биллинг – информация, полученная по техническому каналу связи, включающая в себя периоды времени соединения технических устройств, в том числе и средств информационного обмена, предоставленной услуги осуществления обмена и передачи, объема переданной информации (вне зависимости от ее вида), а также определение места передачи до пункта ее получения.

Процесс (получение) биллинга – определение (установление) по техническому каналу связи периода времени соединения технических устройств, в том числе и средств информационного обмена, предоставленной услуги осуществления обмена и передачи, объема переданной информации (вне зависимости от ее вида), а также определение места передачи до пункта ее получения.

БИН (BIN) – первые шесть цифр номера банковской карты; расшифровывается данная аббревиатура как «банковский идентификационный номер».

Блокирование информации – действие, искусственно затрудняющее доступ пользователей к компьютерной информации, не связанное с ее уничтожением, а также создающее условия (в том числе с помощью специальных программ), исключающие использование компьютерной информации ее законным владельцем.

Виртуальная личность – совокупность данных, характеризующих пользователя и представляющих его в Интернете: логин, фотоизображение, почтовый адрес, подпись на форуме.

Виртуальная машина – программа, которая эмулирует реальный (физический) компьютер со всеми его компонентами (жесткий диск, привод, сетевые адаптеры и прочее).

Виртуальный сервер – услуга по предоставлению в аренду так называемого виртуального выделенного сервера. В плане управления операционной системой по большей части она соответствует физическому выделенному серверу.

Виртуальная частная сеть (VPN) – обобщенное название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) «поверх» другой сети (например, Интернет).

Выемка – следственное действие, направленное на добровольное либо принудительное изъятие дознавателем, следователем материальных объектов и (или) документов из законного или незаконного владения у граждан, учреждений, организаций, предприятий. Выемка проводится в случае необходимости изъятия определенных предметов, имеющих значение для уголовного дела, если точно известно, где и у кого они находятся. Отличительной особенностью выемки от обыска является запрет на производство каких-либо поисковых действий.

Даркнет (DarkNet) – известен как «Скрытая сеть», «Темный интернет», «Темная сеть» – скрытая сеть, соединения которой устанавливаются только между доверенными узлами (пирами), иногда именующимися как «друзья», с использованием нестандартных транспортных протоколов и портов. Анонимная сеть представляет собой не связанные между собой виртуальные туннели, представляющие передачу данных в зашифрованном виде. Файлообмен происходит анонимно (поскольку IP-адреса недоступны публично), и, следовательно, пользователи могут общаться без особых опасений и государственного вмешательства. Можно сказать, что это инструмент для осуществления коммуникации в различной неправомерной и незаконной деятельности.

Деанонимизация – совокупность действий, совершаемых лицом или автоматизированной системой, направленных на раскрытие реальной личности пользователя и характеристик его устройств.

Дроп (мул) – лицо, непосредственно осуществляющее обналичивание похищенных денег, снимающее денежные средства с банковской карты и других платежных систем, ранее переведенные со счета жертвы, за определенное денежное вознаграждение.

Дроповод – руководитель дропов, является администратором, отвечающим за направление денежных средств, полученных преступным путем, в адрес организатора преступления.

Залив – перевод денежных средств со счета клиента банка либо со счетов самого банка на реквизиты, заранее подготовленные злоумышленником.

Заливщик – лицо, осуществляющее непосредственное хищение денежных средств клиентов банков.

Злоумышленник (личность преступника) – лицо, обладающее совокупностью социально-психологических свойств и качеств, являющихся причинами и условиями совершения преступлений.

Интернет – всемирная информационная компьютерная сеть, связывающая между собой как пользователей компьютерных сетей, так и пользователей индивидуальных компьютеров для обмена информацией.

IP-адрес (ай-пи адрес, сокращение от англ. *Internet Protocol Address*) – сетевой адрес узла в компьютерной сети, построенной по протоколу IP. При связи через сеть Интернет требуется глобальная уникальность адреса, в случае работы в локальной сети требуется уникальность адреса в пределах сети.

IP-телефония – голосовая связь, осуществляемая по сетям передачи данных, в частности по IP-сетям (IP-Internet Protocol). На сегодняшний день IP-телефония все больше вытесняет традиционные телефонные сети за счет легкости развертывания, низкой стоимости звонка, простоты конфигурирования, высокого качества связи и сравнительной безопасности соединения.

IP-телефония – это общий термин, обозначающий передачу голоса и факса, а также связанные с этим сервисы, частично или полностью, через пакетные сети на основе протокола IP (Internet Protocol – протокол межсетевое взаимодействия).

Термин «IP-телефония» эквивалентен термину «VoIP» (Voice over IP). Internet-телефония – более узкое понятие, когда в роли транспортной среды выступает сеть Internet.

Кардинг (англ. *carding*) – род мошенничества (самый вредоносный вид хакерства), при котором производится операция с использованием банковской карты или ее реквизитов, не инициированная или не подтвержденная ее держателем. Реквизиты платежных карт, как правило, берут со взломанных серверов интернет-магазинов, платежных и расчётных систем, а также с персональных компьютеров (либо непосредственно, либо через программы удаленного доступа, так называемые «трояны» и «черви»).

Кардселлер – лицо, осуществляющее приобретение банковских карт с последующей перепродажей с целью наживы (покупает за меньшую цену и перепродает дроповоду за повышенную цену).

Киберпреступность – совокупность преступлений, совершаемых в киберпространстве с помощью или посредством компьютерных систем или компьютерных сетей, а также иных средств доступа к киберпространству в рамках компьютерных систем или сетей, а также против компьютерных систем, компьютерных сетей и компьютерных данных.

Таким образом, понятие «киберпреступление» не ограничивается только рамками сети Интернет, оно распространяется на все виды преступлений, совершаемых в информационно-телекоммуникационной сфере¹.

Несанкционированный доступ к информации – доступ к информации, хранящейся на различных типах носителей (бумажных, магнитных, оптических и т. д.) в компьютерных базах данных, файловых хранилищах, архивах, секретных частях и т. д. различных организаций путём изменения (повышения, фальсификации) своих прав доступа.

Объект деанонимизации – объект, персональные данные которого опубликованы в сети Интернет, тот объект, деанонимизацию которого осуществляют.

Обыск – действие, относящееся к разряду следственных, направленное на принудительное обследование участков местности, жилищ, предметов и документов по отысканию объектов, имеющих отношение к расследуемому преступному событию, а также обнаружению лиц, скрывающихся от правосудия, и объектов, запрещенных соответствующим законодательством в свободном обороте.

Организатор – лицо, осуществляющее координацию преступных действий со стороны участников преступной группы и распределение ролей между указанными лицами, а также определение последующих выплат денежных средств, добытых участниками преступной группы.

Осмотр – самый распространенный метод обнаружения путем восприятия должностным лицом улик-объектов, которые впоследствии могут быть признаны доказательством в ходе расследования того или иного преступления. Данное действие является единственным, которое законодатель позволяет проводить как до момента возбуждения уголовного дела, так и после него.

Платежная система сети Интернет («электронный кошелек») – система расчетов между финансовыми организациями, бизнес-организациями и интернет-пользователями при купле-продаже товаров и за различные услуги через Интернет.

¹ Чекунов И. Г. Киберпреступность: понятие и классификация // Российский следователь. – 2012. – № 2. – С. 37.

Преступления прошлых лет – преступления, совершенные, зарегистрированные, по которым возбуждены уголовные дела, а затем приостановлены за неустановлением лица, виновного в совершении преступления; сроки давности привлечения лица к уголовной ответственности за совершение данного преступления не истекли.

Латентные преступления – совершенные преступления, информация о которых не дошла по каким-либо причинам до регистрации в органах внутренних дел, но относящиеся к перечню, указанному в Особенной части УК РФ.

Скимминг – снятие информации с финансового инструмента пользователя с целью последующего хищения денежных средств и других противоправных действий.

Скриншот – мгновенный снимок экрана, осуществляемый нажатием клавиши «PrtScr» на клавиатуре.

Цифровизация – новый этап автоматизации и информатизации в деятельности правоохранительных органов, проводимый от имени государства и общества, сущностью которого является процесс перехода к использованию возможностей современных цифровых технологий, а также накопление, систематизация, анализ и хранение полученной оперативно значимой информации в целях дальнейшего использования и прогнозирования оперативно-розыскной и следственной ситуаций специально допущенными лицами для выявления, предупреждения, пресечения, раскрытия и расследования преступлений.

Введение

Преступления, совершаемые в современном информационном пространстве с использованием возможностей сети Интернет, являются одними из самых актуальных и непредсказуемых вызовов со стороны преступных элементов. Противостоять данному явлению возможно только лишь, объединив усилия всех заинтересованных ведомств как на национальном, так и на международном уровнях, а также принимая нестандартные совместные решения в зависимости от сложившейся ситуации.

В этих целях руководство страны и Министерства внутренних дел Российской Федерации постоянно наращивают усилия и создают универсальный международно-правовой механизм, способный противостоять современным видам преступлений, совершаемых в информационном пространстве с использованием возможностей сети Интернет.

Сотрудники правоохранительных органов Российской Федерации на протяжении ряда лет все чаще сталкиваются с трансформирующимися киберугрозами. В связи с этим на различных уровнях проводятся всероссийские и международные конференции и мероприятия, направленные на активизацию борьбы совместными усилиями с преступлениями в сети Интернет. Так, 24–26 июля 2025 г. в г. Санкт-Петербурге состоялась *Международная конференция «ICT-Crime 25», посвященная актуальным вопросам противодействия преступлениям, совершаемым с использованием информационно-коммуникационных технологий* (далее – ИКТ). В данной конференции приняли активное участие ведущие специалисты, деятельность которых связана с решением различного рода вопросов, направленных на своевременное выявление и изобличение преступлений, совершаемых в современном информационном пространстве с использованием возможностей сети Интернет.

Лейтмотивом данной конференции явилось желание участников поделиться новыми идеями и разработками, способствующими дать должный отпор киберпреступникам.

Так, статс-секретарь, заместитель директора Федеральной службы по финансовому мониторингу Г. Ю. Негляд в своем выступлении отметил следующее: «Информационные технологии применяются при совершении самых разных финансовых преступлений. Так, для отмыwania «грязных» денег злоумышленники используют виртуальные активы, в том числе криптовалюты. Возрастают риски вовлечения граждан, в особенности молодежи, в противоправную деятельность в качестве дропов. Можно сказать, что ИКТ, в том числе искусственный интеллект, стали неотъемлемым инструментом преступников в этих и многих других схемах. В таких условиях компетентным органам необходимо пересматривать подходы в борьбе с отмеченными рисками, действовать на опережение. Безусловно, эта работа

активно ведется, процесс цифровизации органов власти носит беспрецедентно масштабный характер».

Глобализация преступности требует от нас постоянного совершенствования методологической и технологической базы, при этом приоритетом должно оставаться неукоснительное соблюдение национальных интересов и защита суверенитета Российской Федерации. Наша задача – создавать и развивать собственные цифровые решения и стандарты, способные эффективно противостоять современным вызовам и обеспечивать безопасность государства и защиту интересов граждан в цифровую эпоху².

Одним из активных участников указанной международной конференции являлся модератор сессии «Наилучшие практики противодействия ИКТ-преступности», заместитель начальника отдела Следственного комитета Российской Федерации Т. Ю. Салихов. В своем докладе он отметил: «Внедрение современных цифровых решений является ключевым фактором обеспечения эффективности расследования как кибер-, так и традиционных преступлений. Комплексная цифровая трансформация, предполагающая развитие систем искусственного интеллекта, внедрение передовых средств видеоаналитики, а также повышение качества работы с большими данными открывают нам новые возможности для повышения доказательственной базы и профилактики преступлений в деятельности правоохранительных органов. В условиях стремительного увеличения объема обрабатываемых данных в ближайшие десятилетия представители правоохранительных органов, в том числе Российской Федерации, будут широко использовать инструменты искусственного интеллекта и робототехники для обеспечения общественной безопасности и противодействия преступности. При этом, каким бы современным ни был уровень технологического развития, система искусственного интеллекта рассматривается исключительно в качестве эффективного помощника следователя, способствующего повышению эффективности раскрытия преступлений, но не заменяющего профессионализм и опыт сотрудников правоохранительных органов»³.

В продолжение сказанному выступил член межведомственной рабочей группы Российской Федерации по противодействию информационной преступности А. О. Вихляев, отметивший, что «машинное обучение, искусственный интеллект, робототехника и новые продукты в сфере высоких технологий становятся основой роста экономики. Данные продукты

² Стрельцов И. А. – заместитель руководителя Главного управления криминалистики Следственного комитета Российской Федерации – руководитель технико-криминалистического управления, генерал-майор юстиции.

³ Салихов Т. Ю. – модератор сессии «Наилучшие практики противодействия ИКТ-преступности» Международной конференции «ICT-Crime 25», заместитель начальника отдела Следственного комитета Российской Федерации.

создают новые возможности для обеспечения безопасности, а цифровые платформы и электронный документооборот кардинально повышают эффективность работы различных организаций, предприятий, социальных и образовательных учреждений, облегчают решение множества бытовых задач. При этом такое повсеместное влечение информационно-коммуникационных технологий создало повышенный интерес к информационной инфраструктуре со стороны злоумышленников. Они рассматривают информационно-коммуникационные технологии не только как объекты, на которые возможны преступные посягательства, но и как новые инструменты совершения противоправных деяний. Современная информационная инфраструктура позволяет злоумышленникам, в том числе из других стран, быстро, дистанционно и с более высоким уровнем анонимности подготавливать и совершать различные виды преступлений. В этой связи компетентным государственным органам совместно с технологическими предприятиями и научным сообществом предстоит находить новые решения, позволяющие повышать эффективность выявления и пресечения преступлений на ранней стадии их подготовки в целях недопущения нанесения никакого вреда и ущерба от противоправных действий злоумышленников. Для успешного решения задач по противодействию таким преступлениям также необходимо постоянно совершенствовать международное сотрудничество в этой сфере»⁴.

В настоящее время быстроразвивающаяся в современном информационном пространстве сеть Интернет дает возможность всем гражданам мирового общества оперативно решать свои вопросы, обмениваться необходимой информацией и ускорять в целом жизненно важные процессы. К нашему сожалению, информационное пространство, куда входит и глобальная сеть Интернет, все активнее стали использовать в своих преступных целях и противоправные элементы. В связи с этим представляем статистические сведения о зарегистрированных преступлениях, совершаемых в современном информационном пространстве с использованием сети Интернет⁵ (см. диагр. 1).

⁴ Вихляев А. О. – член межведомственной рабочей группы Российской Федерации по противодействию информационной преступности.

⁵ *Противоправные элементы* – лица или группы лиц, которые совершают действия, нарушающие закон (противоправные деяния).

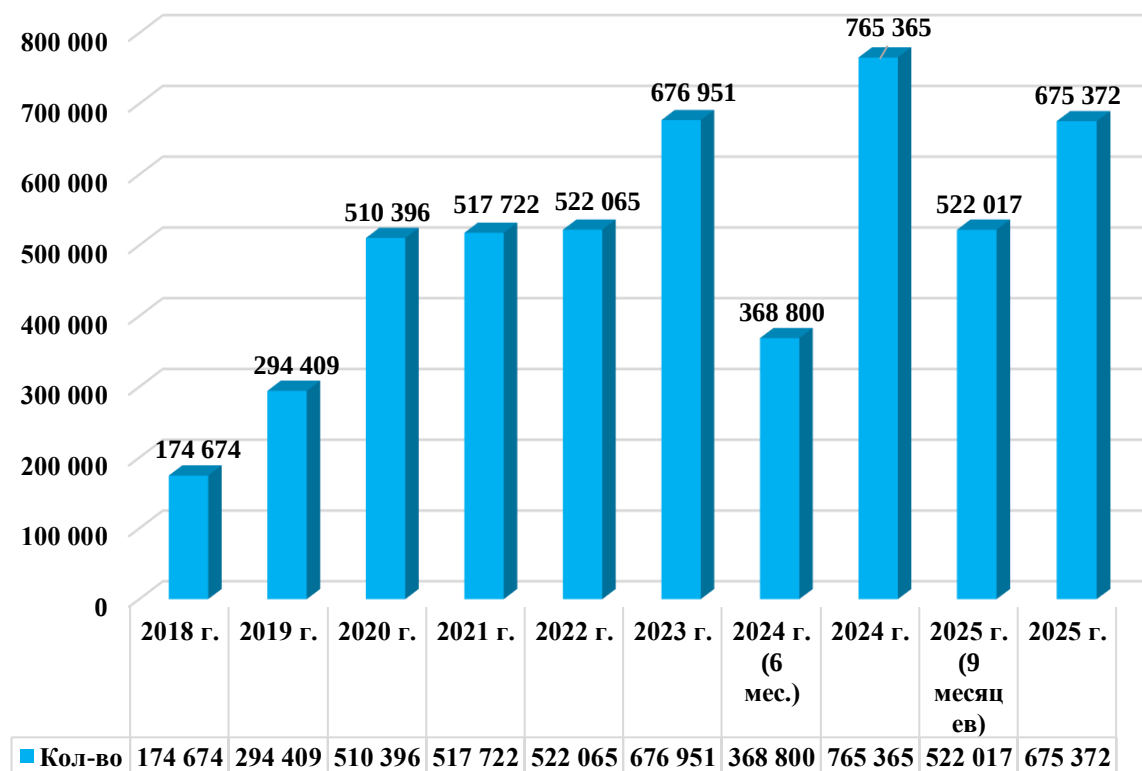


Диаграмма 1. Сведения о количестве зарегистрированных преступлений в сфере информационно-телекоммуникационных технологий за период с 2018 по 2025 год

29 мая 2024 г. состоялось расширенное заседание Совета по стратегическому развитию и нацпроектам и комиссий Госсовета по направлению социально-экономического развития страны, на котором Президент Российской Федерации В. В. Путин дал поручение рассмотреть вопросы развития необходимой информационно-технологической и телекоммуникационной инфраструктуры противодействия информационным угрозам и кибермошенничеству для устойчивого, безопасного и целостного функционирования на территории Российской Федерации информационно-телекоммуникационной сети Интернет.

По этому поводу «в конце июля 2024 г. генеральный прокурор Российской Федерации Игорь Краснов рассказал, что транснациональный характер информационных угроз не оставляет сомнений в необходимости консолидации усилий всех стран для эффективной борьбы с ними. Сейчас не существует глобального международного договора в данной сфере, и преступники всех мастей, зная об этом, действуют, не опасаясь ответственности. По мнению Генерального прокурора Игоря Краснова, таким инструментом под эгидой ООН могла бы стать всеобъемлющая международ-

ная конвенция о противодействии использованию информационно-коммуникационных технологий в преступных целях, которая разрабатывается на площадке специального межправительственного комитета ШОС»⁶.

Исходя из складывающейся криминогенной и оперативной обстановки, Президент Российской Федерации В. В. Путин ежегодно проводит в Кремле заседания Совета безопасности, посвященные вопросам противодействия угрозам национальной безопасности в информационной сфере. На повестку дня выдвигаются вопросы актуализации подходов к решению основных задач, определенных Стратегией национальной безопасности⁷, Доктриной информационной безопасности⁸, Указом Президента РФ от 1 мая 2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»⁹, а также вопросы устойчивого функционирования российского сегмента сети Интернет. Путин В. В. выдвигает к рассмотрению приоритетные вопросы, связанные с защитой информационного пространства России от современных угроз, и дает поручения компетентным органам по их решению.

Авторы научно-практического пособия при его подготовке акцентировали свое внимание на особенностях раскрытия преступлений, совершаемых в современном информационном пространстве с использованием сети Интернет.

Представленное научно-практическое пособие разработано с целью повышения квалификации сотрудников оперативно-следственных подразделений органов внутренних дел ГУ МВД России по г. Москве по вопросам выявления и раскрытия преступлений, совершаемых в современном информационном пространстве с использованием сети Интернет, а также направлено на ориентирование сотрудников к творческому и индивидуальному подходу при решении оперативно-служебных задач.

⁶ Путин поручил развивать инфраструктуру по противодействию инфоугрозам // RGRU: [сайт]. – URL: <https://rg.ru/2024/08/06/putin-poruchil-razvivat-infrastrukturu-po-protivodejstviu-infougrozam.html> (дата обращения: 12.09.2025).

⁷ О Стратегии национальной безопасности Российской Федерации до 2020 года: Указ Президента Российской Федерации от 12 мая 2009 г. № 537 // Информационно-правовой портал «Гарант.Ру». – URL: <https://www.garant.ru/products/ipo/prime/doc/95521/> (дата обращения: 12.09.2025).

⁸ Об утверждении Доктрины информационной безопасности Российской Федерации: Указ Президента РФ от 5 декабря 2016 г. № 646 // Информационно-правовой портал «Гарант.Ру». – URL: <https://base.garant.ru/71556224/> (дата обращения: 12.09.2025).

⁹ О дополнительных мерах по обеспечению информационной безопасности Российской Федерации: Указ Президента РФ от 1 мая 2022 г. № 250 // Информационно-правовой портал «Гарант.Ру». – URL: <https://base.garant.ru/404561984/> (дата обращения: 12.09.2025).

Глава 1.
Анализ состояния преступности
в России за 2023–2024 гг.
Общие понятия
современного информационного пространства
и сведения о глобальной сети Интернет

Анализируя криминогенную обстановку и основываясь на краткой характеристике состояния преступности в Российской Федерации за январь–декабрь 2023 г., можно сделать следующий вывод.

За 2023 год зарегистрировано 1 947,2 тыс. преступлений, или на 1,0 % меньше, чем за аналогичный период прошлого года. Рост регистрируемых преступлений отмечен в 40 субъектах Российской Федерации, что указывает на снижение количества преступлений в 45 субъектах.

Органами внутренних дел выявляется 92,8 % всех зарегистрированных преступлений, причем благодаря своевременно полученной оперативно-розыскной информации 6,1 % из них – на стадиях приготовления и покушения. Всего на этих стадиях выявлено 110,6 тыс. преступлений (+10,9 %).

Четыре преступления из пяти (82,9 %) регистрируются в городах и поселках городского типа – всего 1,6 млн, шестая часть (16,5 %) – в сельской местности, где зарегистрировано 321,5 тыс. преступлений, что на 7,2 % меньше, чем за январь–декабрь 2022 г.

В результате преступных посягательств погибло 21,0 тыс. человек, тяжкий вред здоровью причинен 32,4 тыс. человек.

Ущерб от преступлений (по оконченным и приостановленным уголовным делам) составил 587,6 млрд руб., что на 21,5 % меньше аналогичного показателя прошлого года. Причем более чем три четверти ущерба (84,4 %) приходится на преступления, зарегистрированные в городах и поселках городского типа.

Удельный вес тяжких и особо тяжких преступлений в числе зарегистрированных возрос с 27,3 % в январе–декабре 2022 г. до 30,3 %.

Больше половины всех зарегистрированных преступлений (53,5 %) составляют хищения чужого имущества, совершенные путем: кражи – 583,3 тыс. (–16,4 %), мошенничества – 433,7 тыс. (+26,4 %), грабежа – 22,2 тыс. (–23,9 %), разбоя – 3,4 тыс. (–15,4 %). Почти каждая седьмая кража (13,3 %), каждый двадцать седьмой грабеж (3,7 %) и почти каждое седьмое разбойное нападение (13,5 %) были сопряжены с незаконным проникновением в жилище, помещение или иное хранилище.

В январе–декабре 2023 г. зарегистрировано 20,5 тыс. квартирных краж, что на 24,6 % меньше по сравнению с аналогичным периодом 2022 года. Данное снижение количественных показателей говорит об активизации деятельности оперативного состава сотрудников органов

внутренних дел, благодаря чему лица, склонные к совершению подобного рода преступлений, были своевременно изобличены, в отношении них проведена работа соответствующего характера.

Количество выявленных преступлений, связанных с незаконным оборотом оружия, по сравнению с январем–декабрем 2022 г. сократилось на 12,8 % и составило 19,4 тыс., а количество выявленных фактов хищения и вымогательства оружия, боеприпасов, взрывчатых веществ и взрывных устройств сократилось на 31,5 % (578 преступлений).

В январе–декабре 2023 года с использованием оружия, боеприпасов, взрывчатых веществ, взрывных или имитирующих их устройств совершено 5,7 тыс. преступлений (–7,9 %).

Более трети (34,8 %) зарегистрированных в 2023 году преступлений совершено в современном информационном пространстве с использованием сети Интернет (всего 677,0 тыс.; +29,7 %). В общем числе зарегистрированных преступлений их удельный вес увеличился с 26,5 % в 2022 году до 34,8 %.

Больше половины таких преступлений (50,6 %) относятся к категориям тяжких и особо тяжких (342,6 тыс.; +25,9 %), более чем три четверти (77,8 %) совершено с использованием сети Интернет (526,8 тыс.; +38%), почти половина (44,7 %) – с использованием средств мобильной связи (302,9 тыс.; +42,2 %).

Почти две трети таких преступлений (70,2 %) совершено путем кражи или мошенничества – 475,3 тыс. (+28,1 %), почти каждое восьмое (12,0 %) – с целью незаконного производства, сбыта или пересылки наркотических средств – 81,5 тыс. (+31,0%).

Проведенный анализ оперативно-служебной деятельности сотрудников оперативных и следственных подразделений органов внутренних дел позволяет сделать вывод о том, что в большинстве случаев лица, совершившие указанные преступления, прибегали к использованию возможностей современной информационно-коммуникационной среды.

Рассматривая криминогенную обстановку и основываясь на краткой характеристике состояния преступности в Российской Федерации за январь–декабрь 2024 г., можно сделать следующий вывод.

В январе–декабре 2024 г. зарегистрировано 765,4 тыс. преступлений, совершаемых с использованием информационно-телекоммуникационных технологий (далее – ИТТ) или в сфере компьютерной информации, что на 13,1 % больше, чем за аналогичный период прошлого года (677,0 тыс. преступлений). В общем числе зарегистрированных преступлений их удельный вес увеличился с 34,8 % в январе–декабре 2023 года до 40 %.

Практически все такие преступления (98,7 %) выявляются органами внутренних дел.

Почти половина подобных преступлений (48,2 %) относятся к категориям тяжких и особо тяжких (369,3 тыс.; +7,8 %), четыре преступления из пяти (84,8 %) совершаются с использованием сети Интернет (649,1 тыс.; +23,2 %), почти половина (45,2 %) – средств мобильной связи (346,0 тыс.; +14,3 %).

Почти две трети таких преступлений (63,5 %) совершается путем кражи или мошенничества – 486,3 тыс. (+2,3 %), почти каждое восьмое (12,4 %) – с целью незаконного производства, сбыта или пересылки наркотических средств – 94,6 тыс. (+16,1 %).

В январе–декабре 2023 г. зарегистрировано 677, 0 тыс. преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, что на 29,7 % больше, чем за аналогичный период прошлого года. В общем числе зарегистрированных преступлений их удельный вес увеличился с 26,5 % в январе–декабре 2022 г. до 34,8 %.

Практически все такие преступления (98,8 %) выявляются органами внутренних дел.

Больше половины таких преступлений (50,6 %) относится к категориям тяжких и особо тяжких (342,6 тыс.; +25,9 %), более чем три четверти (77,8 %) совершаются с использованием сети Интернет (526,8 тыс.; +38,2 %), почти половина (44,7 %) – средств мобильной связи (302,9 тыс.; +42,2 %).

Почти две трети таких преступлений (70,2 %) совершается путем кражи или мошенничества – 475,3 тыс. (+28,1 %), почти каждое восьмое (12,0 %) – с целью незаконного производства, сбыта или пересылки наркотических средств – 81,5 тыс. (+31,0 %).

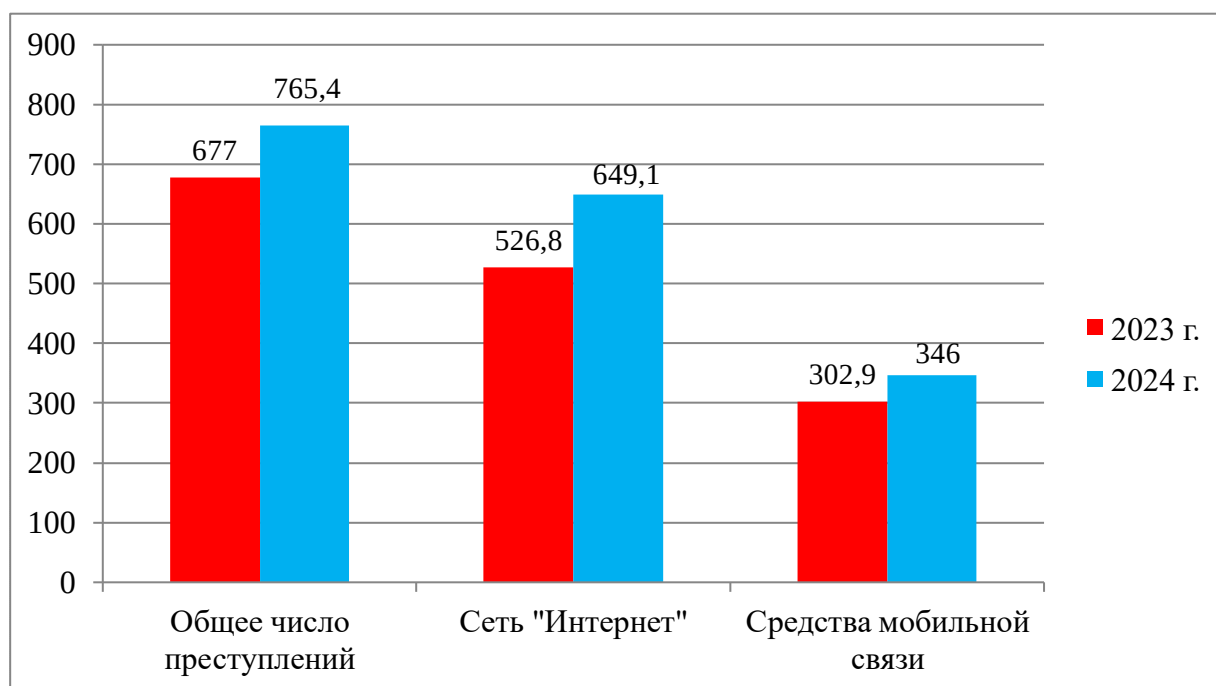


Диаграмма 2. Преступления, совершенные с использованием ИТТ или в сфере компьютерной информации (в сети «Интернет» и с использованием средств мобильной связи)

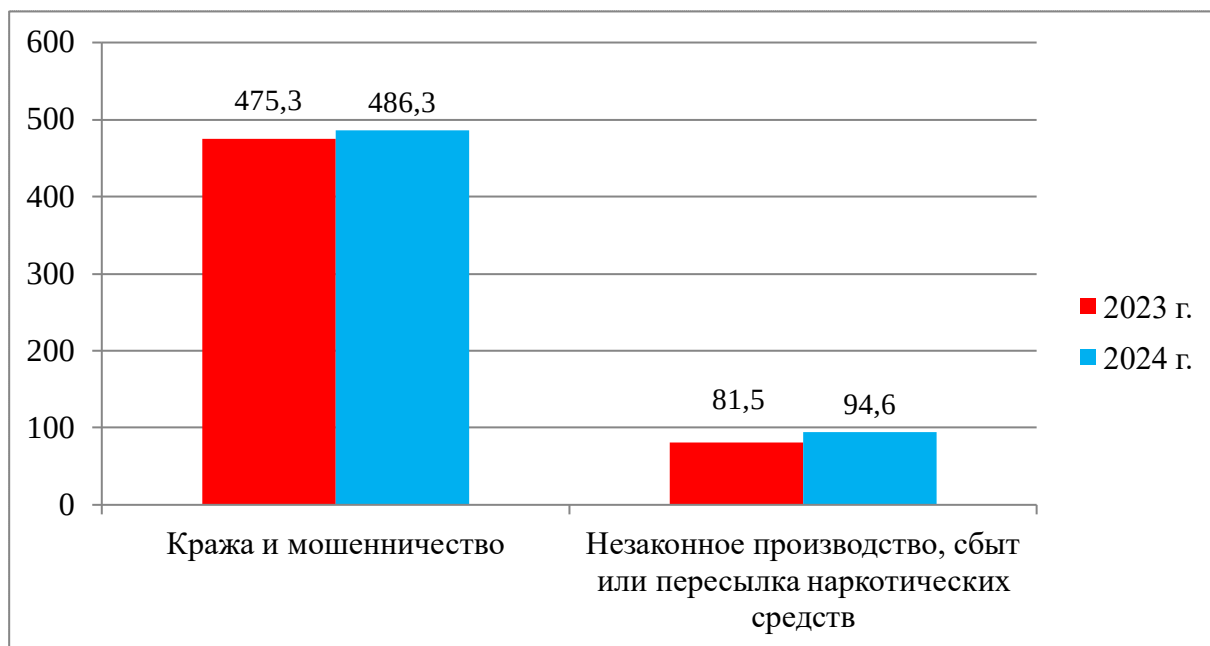


Диаграмма 3. Преступления, совершенные с использованием ИТТ или в сфере компьютерной информации (совершенные путем кражи или мошенничества и незаконного производства, сбыта или пересылки наркотических средств)

В январе–декабре 2024 г. зарегистрировано 1 911,3 тыс. преступлений или на 1,8 % меньше, чем за аналогичный период прошлого года. Рост регистрируемых преступлений отмечен в 28 субъектах Российской Федерации, снижение – в 57 субъектах.

Органами внутренних дел выявлено 91,6 % всех зарегистрированных преступлений, причем 6,7 % из них – на стадиях приготовления и покушения. Всего на этих стадиях выявлено 118,1 тыс. преступлений (+6,8%).

Четыре преступления из пяти (83,4 %) регистрируются в городах и поселках городского типа – всего 1,6 млн, почти шестая часть (15,6 %) – в сельской местности, где зарегистрировано 298,0 тыс. преступлений, что на 7,3 % меньше, чем за январь–декабрь 2023 г.

Удельный вес тяжких и особо тяжких преступлений в числе зарегистрированных возрос с 30,3 % в январе–декабре 2023 г. до 32,3 %.

Больше половины всех зарегистрированных преступлений (50,5 %) составляют хищения чужого имущества, совершенные путем: кражи – 499,6 тыс. (–14,3 %), мошенничества – 445,7 тыс. (+2,8 %), грабежа – 17,6 тыс. 20,7 %), разбоя – 2,8 тыс. (–16,3 %). Почти каждая девятая кража (10,7 %), каждый двадцать седьмой грабеж (3,8 %) и почти каждое седьмое разбойное нападение (13,8 %) сопряжены с незаконным проникновением в жилище, помещение или иное хранилище.

По сравнению с январем–декабрем 2023 г. на 0,2 % возросло число преступлений экономической направленности, выявленных правоохранительными органами, в том числе при проведении оперативно-розыскных мероприятий соответствующего вида. Всего выявлено 105,4 тыс. преступлений данной категории, удельный вес этих преступлений в общем числе зарегистрированных составил 5,5 %.

Материальный ущерб от указанных преступлений (по оконченным и приостановленным уголовным делам) составил 295,7 млрд руб.

Тяжкие и особо тяжкие преступления в общем числе выявленных преступлений экономической направленности составили 64,3 %.

Подразделениями органов внутренних дел выявлено 83,8 тыс. преступлений экономической направленности, их удельный вес в общем массиве преступлений экономической направленности составил 79,5 %.

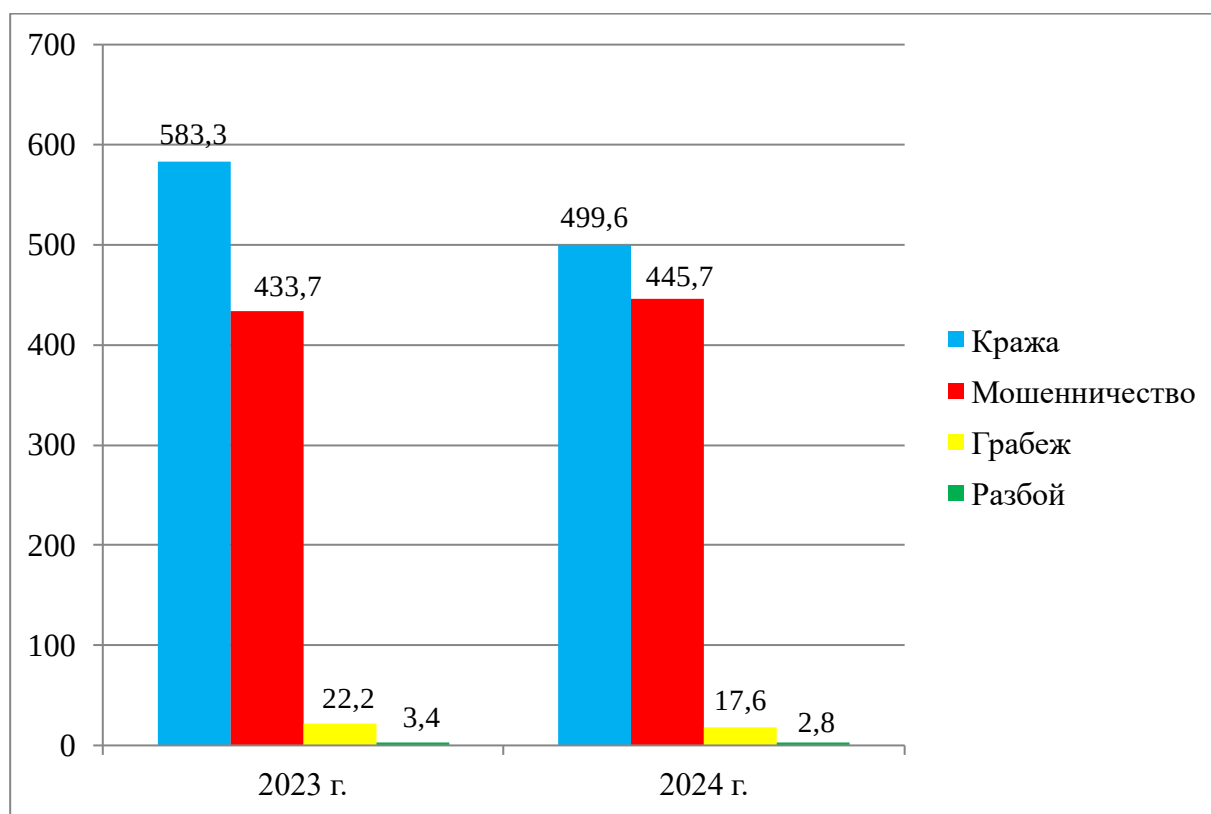


Диаграмма 4. Состояние преступности
(кражи, мошенничества, грабежи, разбои) в 2023, 2024 гг.

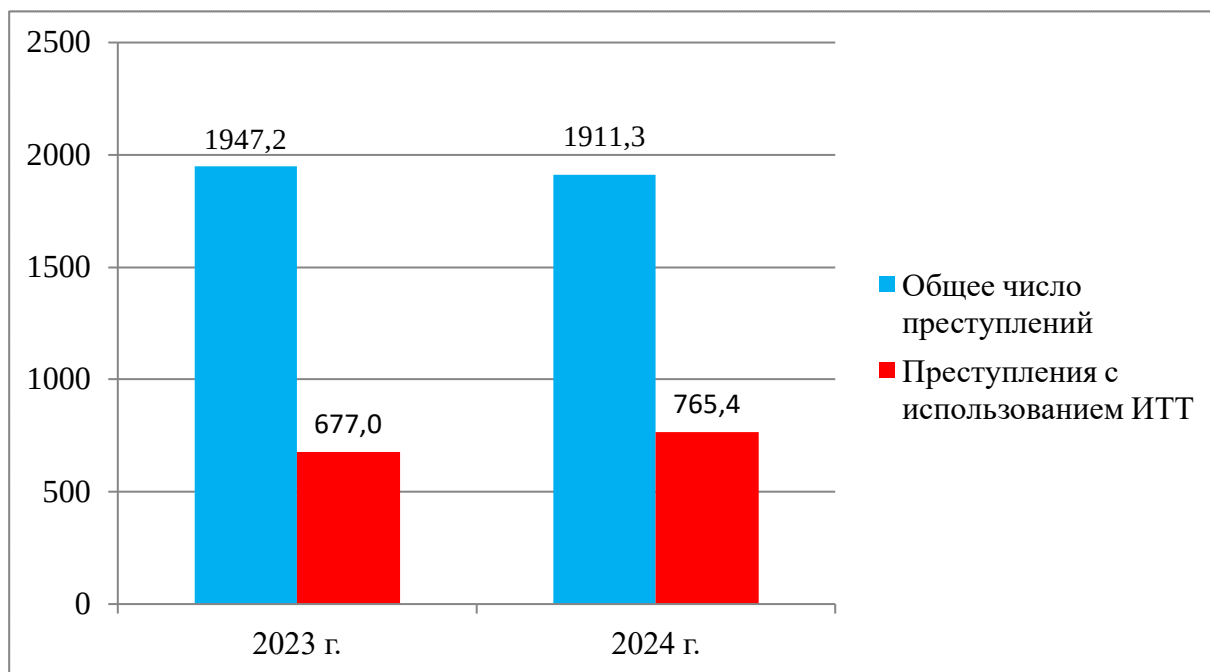


Диаграмма 5. Соотношение общего числа преступлений с преступлениями с использованием ИТТ (2023, 2024 гг.)

В настоящее время анализ складывающейся криминогенной обстановки, а также имеющиеся статистические сведения о совершаемых преступлениях на территории Российской Федерации позволяют сделать вывод о том, что преступления, совершаемые в сфере телекоммуникаций и компьютерной информации, в условиях цифровизации ежегодно имеют тенденцию значительного роста (см. диагр. 1).

Исходя из представленных статистических сведений, можно сделать вывод о том, что проблема противодействия преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий, остается крайне актуальной, требующей особо пристального внимания со стороны правоохранительных органов и государства. Действительно, развитие современного информационного пространства и использование сети Интернет сопровождаются активной деятельностью преступников. Однако проблема заключается не только в увеличении числа преступлений в рассматриваемой сфере, но и в повсеместном распространении таких преступлений во всех областях жизнедеятельности граждан Российской Федерации. Новейшие современные компьютерные и информационные технологии используются при незаконном обороте наркотических средств и психотропных веществ, пропаганде деструктивной идеологии, совершении различного рода мошеннических действий, дистанционных хищений, незаконных финансовых операций и других видов преступлений.

Современное информационное пространство представляет собой совокупность информационных ресурсов, систем и сетей, которые обеспечивают передачу, обработку и хранение информации. Оно отражает социально-экономическую, политическую и культурную жизнь общества. Считаем необходимым обозначить некоторые характеристики современного информационного пространства:

- *доступность* означает, что современные технологии позволяют каждому пользователю иметь доступ к информации, независимо от его местоположения;

- *цифровизация* – с развитием технологий и Интернета все больше пользователей имеют доступ к онлайн-ресурсам. В настоящее время во многих литературных источниках употребляется термин «цифровизация», однако нигде нет его определения. С учетом криминалистического, оперативно-розыскного и следственного аспектов авторы сформулировали определение термина «цифровизация».

Цифровизация – новый этап автоматизации и информатизации в деятельности правоохранительных органов, проводимый от имени государства и общества, сущностью которого является процесс перехода к использованию возможностей современных цифровых технологий, а также накопление, систематизация, анализ и хранение полученной оперативно значимой информации в целях дальнейшего использования и прогнозирования оперативно-розыскной и следственной ситуаций специально допущенными лицами для выявления, предупреждения, пресечения, раскрытия и расследования преступлений»;

- *разнообразие источников информации* свидетельствует о существовании различных источников – печатных изданий, телевидения, радио, Интернета и социальных сетей;

- *роль процесса глобализации* состоит в быстром обмене информацией и позволяет бизнесу в целом и предпринимателям в частности оперативно реагировать на изменения рынка и успешно развиваться.

Каждый пользователь современного информационного пространства может стать и являться его субъектом, имеющим право в своей деятельности создавать новую информацию, накапливать и передавать ее, присваивать и закреплять за собой.

В основе современного информационного пространства лежат различные технологии:

- *искусственный интеллект и машинное обучение* – способность компьютеров обрабатывать большие объемы данных и принимать решения

на основе полученной информации, что открывает возможности для автоматизации процессов в различных отраслях;

– *блокчейн* – технология хранения и передачи данных в виде цепочки блоков. Каждый блок содержит информацию о транзакциях, связан с предыдущим и защищен с помощью криптографии. Данные в блокчейне защищены от изменений и фальсификации. Главная особенность технологии блокчейна – децентрализация, где нет единого контролирующего узла, который может отменить некоторые действия пользователей. Например, банк переводит деньги между счетами двух клиентов. Если перевод покажется банку подозрительным или на счете клиента будет недостаточно средств, банк не проведет операцию. В блокчейне же нет такой «третьей силы, которая стоит над схваткой». Если пользователи договорились и провели перевод, отменить его никто не в силах.

Интернет – это всемирная сеть, объединяющая миллионы устройств посредством кабелей, спутников и других средств связи. Его суть – доступ к информации и сервисам независимо от географического положения пользователей. Интернет начал формироваться в 1969 году с созданием сети АРПАНЕТ (ARPANET), которая объединила несколько компьютеров в США. Ключевым этапом развития стало внедрение в 1983 году протокола ТСР/Р, позволившего различным сетям взаимодействовать друг с другом и ставшего основой современного Интернета. Принцип работы Интернета основан на системе компьютерных сетей, которые связаны друг с другом одинаковыми стандартами и протоколами для обмена данными. Транспортировка информации между разными устройствами происходит посредством кабелей, маршрутизаторов, коммутаторов и серверов, а каждому сайту в Интернете присвоен свой IP-адрес. На 5 января 2025 г. к Интернету подключилось 5,3 млрд пользователей (66 % всего населения земного шара). На сегодняшний день Интернетом пользуются около 5,5 млрд человек (68 % от общего населения Земли), среди которых не только законопослушные граждане, но и те, кто использует возможности современного информационного пространства и сети Интернет в преступных целях.

Авторы научно-практического пособия акцентировали свое внимание на одном из приоритетных направлений в организации деятельности сотрудников органов внутренних Российской Федерации – раскрытии преступлений, совершаемых в современном информационном пространстве с использованием сети Интернет.

Предлагаем рассмотреть некоторые особенности подобных преступлений.

1.1. Сотовая связь и базовые станции

Одним из современных видов преступлений, совершаемых в современном информационном пространстве с использованием сети Интернет, являются дистанционные хищения.

Практика раскрытия и дальнейшее расследование дистанционных хищений показывает, что большинство схем дистанционных мошеннических действий основано 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, обслуживающей абонентов в своей зоне действия.

В настоящее время с учетом быстро развивающихся современных информационных технологий базовые станции устанавливают на крышах высоких зданий, вышках и делят зону их покрытия на три или шесть секторов (рис. 1).

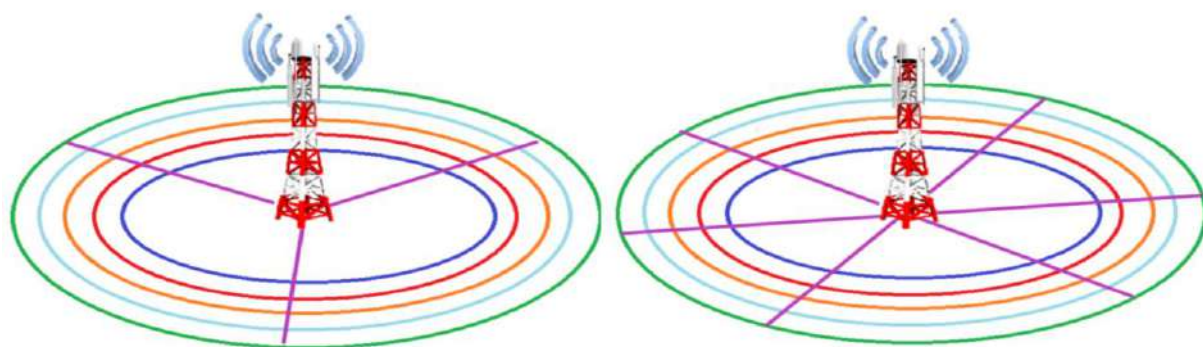


Рис. 1. Базовые станции

Действующие или функционирующие 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 – на расстоянии 100 м друг от друга, в сельской местности – 10–15 км.

В этой связи представляется целесообразным запрашивать у оператора сотовой связи наряду с детализацией телефонных разговоров 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.

1.2. Абонентский номер

Под «абонентским номером» следует понимать номер, идентифицирующий окончательный элемент сотовой связи. Он состоит из 11 последовательных цифр, 1-я из которых определяет код страны, 2, 3, 4-я – принадлежность абонентского номера к региону или оператору сотовой связи, остальные – 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 (прямая ссылка: 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 (рис. 2).

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.

Рис. 2. Установление принадлежности абонентского номера к оператору сотовой связи

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).

1.3. Imei

IMEI (*International Mobile Equipment Identity* – международный идентификатор мобильного оборудования) – уникальный номер сотового аппарата.

Данный номер состоит из 15 последовательных чисел, из которых первые 14 определяют происхождение, модель и серийный номер сотового устройства, а 15-я – 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. Рассмотрим на примере алгоритм определения модели сотового телефона с IMEI 353315071569370 (рис. 3).



Наугад подбираем последнюю контрольную цифру (пока не исчезнет надпись «Invalid IMEI»), нажимаем кнопку «CHECK»



и получаем результат

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

Рис. 3. Определение модели терминала сотовой связи по IMEI

Полная 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. IP-адрес и средство анонимизации сети (VPN)

Сотрудники органов внутренних дел, призванные раскрывать преступления, совершаемые в современном информационном пространстве в сети Интернет, уделяют большое внимание распознаванию схем хищений, посредством которых мошенники своими действиями совершают преступления. В этих целях сотрудники органов внутренних дел через средства массовой информации рассказывают о действиях мошенников, направленных на похищение денежных средств, завладение личной информацией, находящейся в социальных сетях, а также иной конфиденциальной информацией. Они информируют граждан, о том, что необходимо знать в подобных ситуациях, раскрывают некоторые основные понятия, связанные с IT-технологиями. Одним из таких понятий является **IP-адрес**.

IP-адрес (*Internet Protokol address*) – это уникальный идентификационный номер, присваиваемый 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 присваивается 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 (рис. 4).

Компьютер посредством нажатия пользователем клавиши мыши инициирует запрос сайту по протоколу IP



Сайт по протоколу IP предоставляет ответ в виде отобразившейся страницы

Рис. 4. Обмен информацией в сети Интернет

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 сеть Интернет мошенник оставляет свой «след», по которому его можно вычислить (см. рис. 5).



Рис. 5

Так же 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 (прямая ссылка: www.2ip.ru/whois/), зная IP-адрес, можно легко определить провайдера. Рассмотрим на примере IP-адреса 178.218.36.0 (рис. 6).

IP	178.218.36.0
Хост:	178-218-36-0.pppoe.atexplus.net
Город:	Рыбинск 🚩
Страна:	 Russian Federation
IP диапазон:	178.218.32.0 - 178.218.47.255
CIDR:	178.218.32.0/20
Название провайдера:	ATEXS PLUS Ltd

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

Рис. 6. Получение информации по IP-адресу

Отсюда приходим к выводу, что, определив точно IP-адрес и конкретное время его использования в современном информационном пространстве в сети Интернет, оперативный сотрудник или следователь могут установить абонентский номер злоумышленника, с которого он выходил в сеть, адрес расположения устройства доступа в сеть Интернет (домашний WIFI-роутер, сервер, квартира, частный дом или кафе).

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 выходом на сайт подключается к серверу третьего лица, как правило локализованного на территории иного государства. Схематично работа виртуальной частной сети выглядит следующим образом (рис. 7).



Рис. 7. Пример работы виртуальной частной сети

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

О том, каким образом обойти попытку мошенника скрыть себя в сети, рассмотрим подробно в п. 1.8 гл. I «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. По оценкам ПАО «Сбербанка», ущерб от телефонного мошенничества в 2024 году составил почти 300 млрд руб. В 2025 году телефонные мошенники стали звонить россиянам значительно чаще. Причем большинство телефонных звонков производится представителями украинских спецслужб.

«Телефонное мошенничество стремительно развивается, а традиционные методы противодействия уже не справляются со своими задачами. Современные злоумышленники все активнее применяют передовые технологии, в том числе искусственный интеллект, что требует новых, инновационных подходов, основанных на анализе больших данных и машинном обучении. Для ответа на новые вызовы Сбер создает и внедряет эффективные решения, которые позволяют выявлять и предотвращать мошеннические

действия в режиме реального времени, используя передовые методы – от классических алгоритмов до глубоких нейросетевых моделей и поведенческой аналитики. Сбер открыт к международному сотрудничеству и готов делиться своим опытом в борьбе с мошенничеством, способствуя созданию эффективных глобальных мер противодействия¹⁰».

Авторы данной работы, исследовав проблематику столь актуального вопроса, считают, что потенциальным жертвам телефонного мошенничества необходимо помнить, что не следует разговаривать по телефону с неизвестными лицами, а также вести общение посредством различных мессенджеров.

Для **анонимизации** транзакций, совершаемых в современном информационном пространстве с использованием сети Интернет, в системе электронного оборота денежных средств используется сервис, называемый **миксером**.

Технологическая цепочка работы миксера осуществляется следующим образом: средства клиента дробятся (в автоматическом режиме) на мелкие части, после чего эти части смешиваются в случайном порядке с частями других клиентов сервиса. В результате всех операций к конечному получателю приходит заданное количество денежных средств, небольшими партиями от разных случайно выбранных кошельков, принадлежащих сервису. Данную цепочку перечислений и конечного получателя денежных средств видят сотрудники используемого обменного сервиса. Миксер создается заранее сотрудниками обменного сервиса, который является неизменным, однако операции переводов хаотичны и почти не повторяются.

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

- банковские карты;
- расчетные счета;
- электронные кошельки;
- счета абонентских номеров;
- 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

¹⁰ Велигодский С. С. – старший управляющий – директор департамента противодействия мошенничеству ПАО «Сбербанк».

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». Несмотря 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 их принадлежность. Это сделать довольно просто, если вы знаете, что такое **БИН** (рис. 8).



Рис. 8. Пример БИН на банковской карте

БИН банка – банковский идентификационный номер. Это первые шесть цифр номера банковской карты. Есть множество интернет-сервисов, где можно проверить принадлежность банковской карты. Самые распространенные из них – www.binov.net и www.fraudassets.com. Рассмотрим на примере банковских карт № 4890 4900 0000 0000 (сайт www.binov.net) и № 5106 2100 0000 0000 (сайт www.fraudassets.com) (рис. 9).

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

БИН № 489049 принадлежит «Киви Банк», соответственно, все карты, начинающиеся на эти цифры, принадлежат «Киви Банк»

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».
Соответственно, все карты, начинающиеся на эти цифры,
принадлежат банку «Яндекс.Деньги»*

Рис. 9. Информация о принадлежности БИН к конкретной платежной системе

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 неидентифицированный кошелек имеет мало возможностей (хранение – не более 15 000 руб., оборот – не более 40 000 руб. 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:

– 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»;

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

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

– у оператора сотовой связи «Теле2» нет устоявшегося корреспондента, для проведения расчетных операций он может

использовать большое количество сторонних организаций. Информацию о движении денег нужно запрашивать у самого оператора, а после – у корреспондента.

1.6. Интернет-сайт. 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 многое другое.

Часто встречается такая схема мошеннических действий, при которой злоумышленник создает сайты в виде интернет-магазинов, и похищает денежные средства, «продавая воздух» (рис. 10).

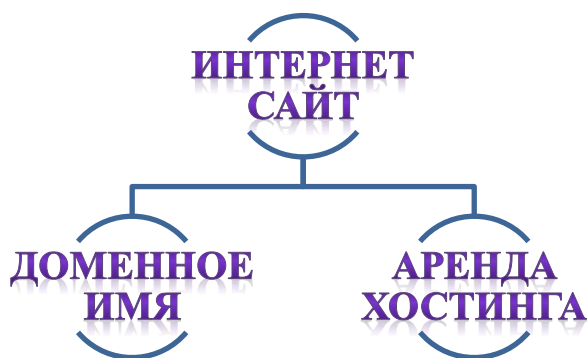


Рис. 10. Схема организации интернет-сайта

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, оплатить предоставляемые услуги. Так как мошенники всегда стараются оставаться в тени, аренду они делают отдаленно – 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.**

Доменное имя. «Доменное имя» – численно-буквенное обозначение, следующее за обозначением всемирной сети («www»). К примеру «vk.com», «youtube.com», «2ip.ru» и др. Доменное имя, так же как и хостинг,

регистрируется у специальных организаций (регистраторов) 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 получить первоначальные сведения по сайту, или WHOIS-сведения. Это довольно просто – в этом нам поможет интернет-ресурс www.reg.ru. Рассмотрим на примере сайта-мошенника www.psou.site (рис. 11).



Рис. 11. Получение информации о домене

Интерес для расследования уголовного дела представляют следующие две графы:

Строка «Registrator», или «регистратор» обозначает данные организации, где было зарегистрировано доменное имя. В случае с сайтом www.psou.site – это ООО «Регистратор доменных имен Рег.Ру». Указанному юридическому лицу следует направлять соответствующий запрос.

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 установили: 1) доменное имя сайта www.psou.site зарегистрировано у организации ООО «Рег.Ру»; 2) у данной организации арендован хостинг.

Кроме того, использованный ресурс 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. рис. 12).

Заходим на сайт www.reg.ru, вводим доменное имя интересующего сайта, нажимаем кнопку «Whois» и получаем нужную информацию:

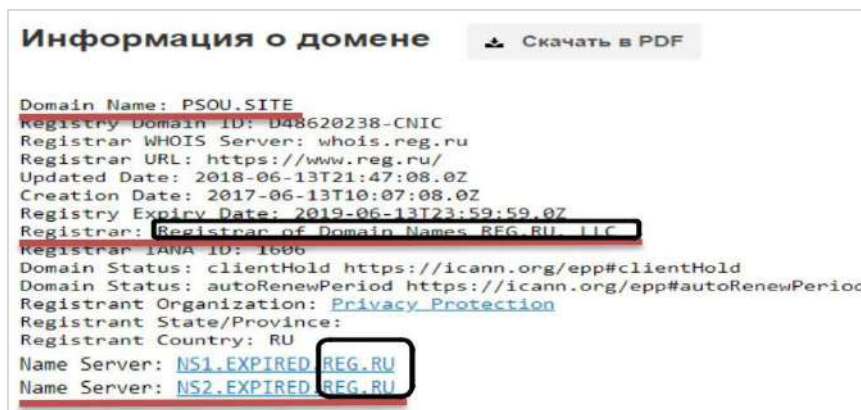


Рис. 12. Информация о домене

1.7. IP-телефония. Звонки в современном информационном пространстве с использованием сети Интернет

Законопослушные абоненты часто встречаются в своей повседневной жизни с абонентскими номерами, которые начинаются на «8 800...». Такие номера представляют SIP-телефонию.

SIP-телефония отличается от обычной 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. п. 1.4 гл. I). Схема связи такого телефонного разговора в упрощенном виде выглядит следующим образом (рис. 13).



Рис. 13. Схема звонка по SIP-телефонии

При этом для звонящего лица 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 SIP-телефонии, используемый мошенником, не имеет физического носителя (сим-карты), он **виртуальный**, при таких обстоятельствах получить информацию в виде привязки к конкретной базовой станции нельзя. Возможно получить лишь сведения об IP-адресах, которые использовал мошенник для подключения к приложению (сайту) по работе с SIP-провайдерами.

Виртуальный номер – это основная услуга SIP-провайдера, работающая через Интернет по принципу переадресации звонков. Виртуальные номера бывают трех видов: номер для приема звонков, номер для приема SMS и номер для приема факса. Каждый имеет свой вид переадресации.

Предлагаем рассмотреть отличительные особенности SIP-телефонии от обычной сотовой телефонной связи:

- 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 абонента;

- **виртуальные номера могут иметь** любой вид, как привычный нам (800) 000-00-00, так и 8 (499) 000-00-00, 8 (475) 20-00-00 и др. В редких случаях – даже абонентские 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 настолько 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; другую значимую информацию, представляющую оперативный интерес.

Осталось ответить на один вопрос – как понять, какому SIP-провайдеру принадлежит тот или иной виртуальный номер? Для этого необходимо воспользоваться ресурсом нумерации «Федерального агентства связи» – www.rossvyaz.ru.

1.8. Cookie-файлы как средства деанонимизации мошенника в современном информационном пространстве с использованием сети Интернет

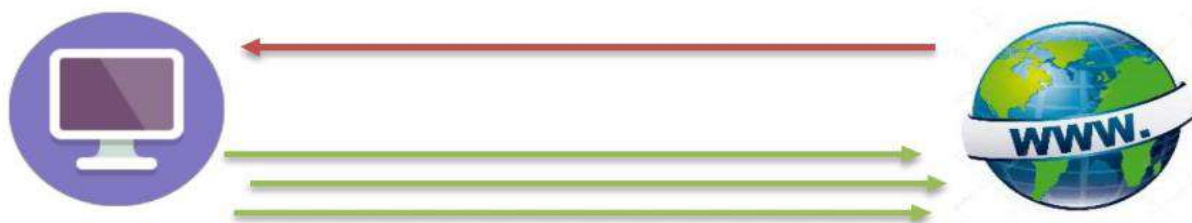
В пункте 1.4 гл. I мы раскрыли понятие IP-адреса и наиболее популярного сервиса анонимизации в современном информационном пространстве с использованием сети Интернет – VPN. Раскроем понятие Cookie-файлов как способа обойти защиту мошенника.

Многие замечали, что стоит внести 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 большое количество 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 информацию, 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;
- предпочитаемый вами язык;
- последние просматриваемые вами страницы;
- историю ваших посещений (данная функция Cookie и имеет для нас ключевое значение).

Схематично Cookie работает следующим образом (рис. 14).



При первом посещении сайта он передает вашему браузеру Cookie-файл.

При всех последующих входах на данный сайт браузер обозначает полученный от него Cookie-файл для идентификации

Рис. 14. Пример работы Cookie

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 Москвы и вносит предоплату на счет указанной банковской карты или абонентского номера, тем самым став жертвой мошеннических действий.

Отправляя 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 **обо 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 И. И. Иванов 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.

Не будем забывать о человеческом факторе: возможно, при создании одного из мошеннических объявлений И. И. Иванов забыл подключиться к VPN.

1.9. Даркнет (DarkNet) как один из элементов сети Интернет

Даркнет (DarkNet, также известен как «Скрытая сеть», «Темный интернет», «Темная сеть») – скрытая сеть, соединения которой устанавливаются только между доверенными узлами (пирами), иногда именуемыми как «друзья», с использованием нестандартных транспортных протоколов

и портов. Анонимная сеть представляет собой систему не связанных между собой виртуальных туннелей, предоставляющих передачу данных в зашифрованном виде. Файлообмен происходит анонимно (поскольку IP-адреса недоступны публично), и, следовательно, пользователи могут общаться без особых опасений и государственного вмешательства. Можно сказать, что это инструмент для осуществления коммуникации в различной неправомерной и незаконной деятельности.

IP-адрес (ай-пи адрес, сокр. от англ. *Internet Protocol Address*) – сетевой адрес узла в компьютерной сети, построенной по протоколу IP. При связи через сеть Интернет требуется глобальная уникальность адреса, в случае работы в локальной сети требуется уникальность адреса в пределах сети.

Когда этот термин используется для описания файлообменной сети, Даркнет часто употребляется в качестве синонимов фразы «Friend to friend» (от друга к другу). Эти два понятия описывают сети, где прямые соединения устанавливаются только между двумя пирами, которые друг другу доверяют. Такие сети по-другому называются «закрытый P2P» (*Private peer to peer*).

Почти все известные даркнеты децентрализованы и, следовательно, считаются одноранговыми.

Одноранговая, децентрализованная или пиринговая (P2P) сеть – оверлейная компьютерная сеть, основанная на равноправии участников. Часто в такой сети отсутствуют выделенные серверы, а каждый узел (пир) является как клиентом, так и выполняет функции сервера. В отличие от архитектуры клиент-сервера такая организация позволяет сохранять работоспособность сети при любом количестве и любом сочетании доступных узлов. Все узлы являются участниками сети (рис. 15).

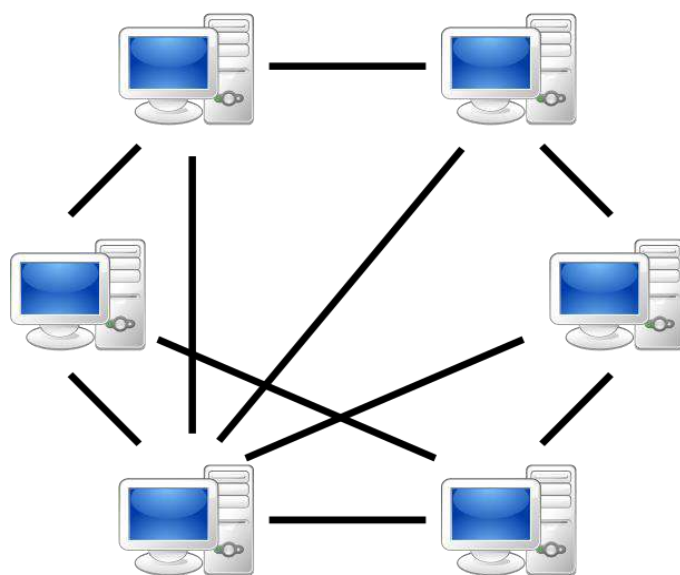


Рис. 15. Одноранговая компьютерная сеть

В даркнете используются домены, на которые невозможно зайти через обычную сеть, используя стандартные браузеры. Зачастую это псевдодомены в доменной зоне .onion или .i2p и др. Для адреса сайта часто используется случайный набор символов или шифр.

Многие теневые сети требуют установки специального программного обеспечения для получения доступа к сети.

Существуют такие популярные теневые сети, как:

- Tor – это одна из самых популярных программ для анонимных сетей, которая также используется для доступа в даркнет;
- I2P;
- RetroShare;
- Freenet;
- GNUnet (при использовании опции «топология F2F»).

Даркнет-рынок, теневой рынок – это коммерческий сайт в даркнете, который работает через Tor или I2P. Они функционируют, в первую очередь, как чёрные рынки, продающие или являющиеся посредниками в сделках с продажей порнографии, наркотиков, кибероружия, оружия, фальшивых денег, поддельных документов, нелегальных фармацевтических препаратов, стероидов и других запрещенных товаров, а также для продажи юридических продуктов (диагр. 6).



Диаграмма 6. Продукты, доступные на даркнет-рынках

Исходя из модели, разработанной Шелковым путём, современные рынки характеризуются использованием тёмного анонимного доступа (как правило, Tor), биткойн-платежей с услугами условного депонирования и систем обратной связи с поставщиками eBay.

Биткойн из-за псевдоанонимности получил широкое распространение для оплат в даркнете. Для повышения уровня анонимности применяют биткойн-миксеры, которые запутывают транзакции, и отследить их манипуляции становится крайне сложно. Большинство биткойн-миксеров дробят средства клиента на мелкие части, после чего эти части смешиваются в случайном порядке с частями других клиентов и рассылаются разным получателям. В результате к конечному получателю приходит заданное количество криптовалюты, но небольшими партиями от разных случайно выбранных адресов из общего пула, принадлежащего сервису.

Блокчейн – выстроенная по определённым правилам непрерывная последовательная цепочка блоков (связный список), содержащих информацию; техническая база для функционирования, в т. ч. криптовалют (но не их одних), способ хранения информации без возможности внесения правок или корректировок в ранее записанные данные.

Блок (составная часть блокчейна) – это составная часть распределённого реестра, представляющая собой набор информации в установленной форме, который содержит в себе данные и хеш-сумму предыдущего блока.

Криптовалюта – разновидность платёжного средства, учёт внутренних расчётных единиц которой обеспечивает децентрализованная платёжная система (нет внутреннего или внешнего администратора или какого-либо его аналога), работающая в полностью автоматическом режиме.

Криптоактивы – основанные на блокчейне системы учёта ценностей. Одна криптовалюта может существовать на разных блокчейнах (например, USDT может быть на блокчейнах Ethereum (ERC-20), Tron (TRC-20), Binance Smart Chain (BSC) и др.). Один блокчейн может быть местом хранения сотен разных криптовалют (например, на ERC-20 существует USDT, BNB, SHIB, DOGE и тысячи других).

На одном адресе в блокчейне может храниться несколько криптовалютных токенов, это чаще всего встречается на распространенных блокчейнах (ERC-20, TRC-20, BSC). Есть блокчейны, где это встречается редко, это или блокчейны со слабо развитой средой для написания смартконтрактов (BTC) или блокчейны, где такой возможности вовсе нет (DASH) (см. рис. 16).

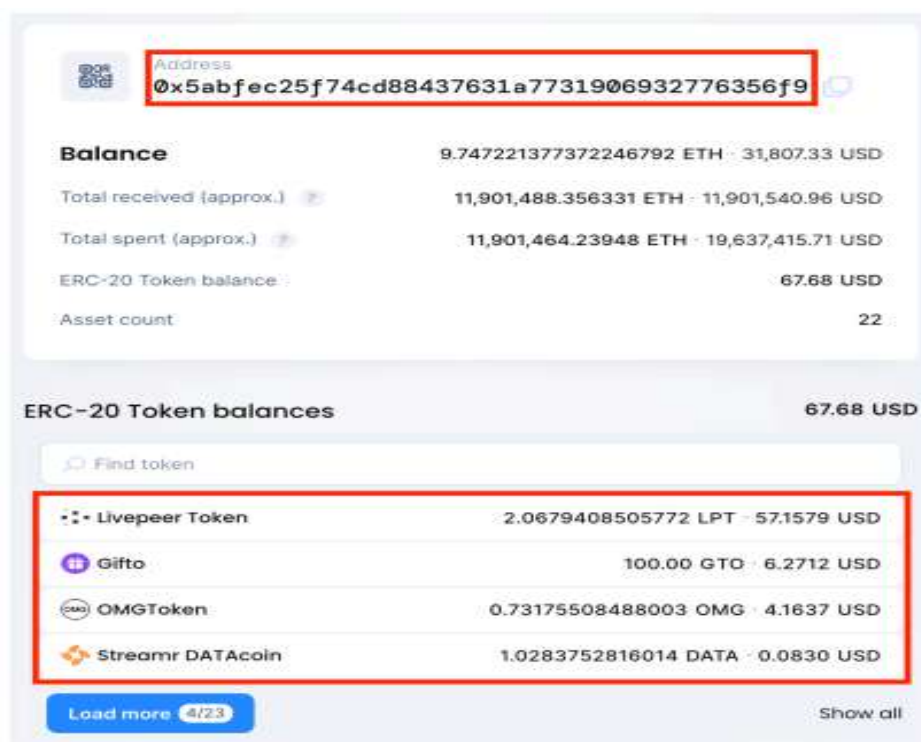


Рис. 16. Соотношение криптовалютного адреса и хранящихся на нем сведений

Криптовалютный адрес – конкретное место хранения криптовалюты в блокчейне.

Кластер (кошелек) – группа адресов, собранная по признаку единого распорядителя.

Кластеризация – процесс объединения криптовалютных адресов в кластеры по определенному автоматическому алгоритму.

Один простой пользователь может, сам того не осознавая, быть обладателем нескольких криптовалютных адресов, которые составляют один кластер. Крупные игроки (биржи, миксеры и т. п.) имеют кластеры на сотни тысяч ассоциированных криптовалютных адресов.

Хеш-идентификатор транзакции (TxID, transaction hash, хеш, хеш-транзакции) – это уникальный (единственный во всем блокчейне) идентификатор конкретной транзакции. Один и тот же адрес может быть получателем и отправителем множества транзакций, но у всех будут разные хеши (см. рис. 17).

Операции				Всего 34
2021-06-20 09:01:47	Тх: 0xb4a67e9d53e377060fe8e37245a52ae8a37ae11b12e906453cd4117750f От: 0xd7b15654191357e078914b9bca4a9c36d7942776 Куда: 0x5abfec25f74cd88437631a7731906932776356f9	Wrapped Satoshi	1,000,000.00 WSAT	
2019-02-20 11:19:10	Тх: 0x8fae4dd4d9161c195e3c2fb3d95d18bcd01d48fa052485e57a929606be43f От: 0x909decd5ed8f7b6168786eff372849c89250b7 Куда: 0x5abfec25f74cd88437631a7731906932776356f9	BigBang Game	10.00 BBGC	
2019-02-20 11:18:11	Тх: 0x1d6256654577b1452ff489b018c4eeea1b172db2a4c2057870360f002c40 От: 0x909decd5ed8f7b6168786eff372849c89250b7 Куда: 0x5abfec25f74cd88437631a7731906932776356f9	BigBang Game	10.00 BBGC	
2018-10-12 19:05:45	Тх: 0x6b8e8471ec2621e862eabb42af736151adae40eb2d61809c5426568017abe От: 0x0000000000000000000000000000000000000000000000000000000000000000 Куда: 0x5abfec25f74cd88437631a7731906932776356f9	Promodl	5 PMOD	
2018-08-17 13:11:28	Тх: 0x1136df18a431c1535432b71fa1861cc44065a685f968032c1374bcd7804a6f От: 0x9cae60996b96219d6675b4a32d05cab2c26c109 Куда: 0x5abfec25f74cd88437631a7731906932776356f9	Bitcoin	1,001.00 BOSS	
2018-08-14 20:21:56	Тх: 0xc344390f9be5e401016850fa1dc94dc96e5d3fb8c71677ec11794c77cc697 От: 0xc7304352548c19216ba59ee15e3e1ae9a5605608 Куда: 0x5abfec25f74cd88437631a7731906932776356f9	GSENetwork	9.00 GSE \$ 0.00 (-99.31%) -\$ 0.06 @ 0.01	

Рис. 17. Хеш-транзакции

Холодный адрес (кошелек) – адрес, приватные ключи от которого (и, как следствие, – право распоряжаться активами на адресе) хранятся у самого пользователя.

Горячий адрес (кошелек) – адрес, приватные ключи от которого хранятся у одного из доверенных лиц, не являющегося владельцем активов на адресе (например, у криптовалютной биржи или онлайн-кошелька криптовалют).

Пока средства находятся на холодном адресе и не имеется доступа к приватному ключу, обращение каких-либо взысканий или блокировка распоряжения средствами на адресе невозможна технически.

Все централизованные криптовалютные биржи (которых на рынке большинство) хранят средства пользователей на своих горячих адресах, проводят (в той или иной степени) процедуру идентификации своих пользователей и ведут логи активности пользователей.

Децентрализованные криптовалютные биржи (DEX) не хранят средства пользователей, пользователи сами осуществляют транзакции со своих холодных адресов, при этом многие из них имеют логи активности

своих пользователей. Каждая биржа имеет собственный порядок предоставления сведений, некоторые вовсе не отвечают на запросы из России.

В этих целях необходимо получить доказательства, и к одним из распространенных способов следует отнести:

- показания участников уголовного процесса;
- осмотр устройств и документов;
- получение ответов от организаций;
- межведомственное взаимодействие;
- международное сотрудничество;
- специальное исследование информации в блокчейне.

Особенности допросов:

- при отправке криптовалюты с биржи – максимально полно зафиксировать данные аккаунта на бирже;
- по возможности приложить скриншоты совершения исходящих платежей с биржи, историю пополнения средств на этой бирже;
- при отправке криптовалюты с холодного кошелька – установить, каким программным обеспечением пользовалось лицо;
- в обоих случаях – установить, каким образом осуществлялась транзакция (само лицо отправило активы или третьими лицами был получен доступ к управлению активами, иным образом);
- зафиксировать суммы транзакций с указанием криптовалюты платежей, даты, времени, криптовалютного адреса получателя средств, а также по возможности указать хеш-идентификатор и криптовалютный адрес отправителя средств.

Особенности назначения специального исследования:

- должны быть точно перечислены реквизиты (криптовалютные адреса, хеш-идентификаторы транзакций и прочее);
- вопросы должны содержать интересующий период, за который нужно изучить блокчейн;
- необходимо поставить вопрос о поступлении средств на криптовалютные адреса, ассоциируемые с централизованными криптовалютными биржами;
- необходимо получить информацию о программном обеспечении, используемом при проведении специального исследования и номере его лицензии;
- дополнительно следует указать на необходимость визуализации предоставленной информации при наличии к тому технической возможности.

Отмывание денежных средств. «Обеление» криптовалютных активов осуществляется с использованием следующих сервисов:

- через криптовалютные мосты;
- обналичивание через криптовалютные обменники, принимающие грязные активы;
- отмывание через биржи, не проводящие AML-проверки;
- «обеление» преступных доходов через децентрализованные площадки.

Способы хищения криптовалютных активов:

- социальная инженерия;
- фишинг (подмена адреса сайта);
- компьютерные вирусы;
- рассылка вредоносных NFT;
- неправомерный доступ к мобильным устройствам;
- технические уязвимости в коде;
- финансовые пирамиды и скам-проекты;
- прошивка аппаратных кошельков;
- смарт-контракты и NFT;
- оффлайн.

Глава 2.
Алгоритм действий
сотрудников следственно-оперативной группы
и дежурных частей
при поступлении сообщения о преступлении,
совершенном в современном
информационном пространстве
с использованием сети Интернет¹¹

2.1. Действия сотрудников дежурных частей
при получении заявления (сообщения) о преступлении,
совершенном в современном информационном пространстве
с использованием сети Интернет

При поступлении заявления, сообщения о преступлении, совершенном в современном информационном пространстве с использованием сети Интернет, в частности о дистанционном хищении, сотрудник дежурной части производит все необходимые действия, предусмотренные нормативными правовыми актами, регламентирующими порядок приема, регистрации и разрешения в органах внутренних дел заявлений, сообщений и иной информации о происшествиях:

1. Выясняет у заявителя путем опроса место и обстоятельства преступления, абонентские номера, с которых заявителю поступили звонки либо смс-сообщения, а также на которые перечислялись денежные средства.

2. Организует незамедлительно выезд на место происшествия (в случае установления) дежурной следственно-оперативной группы (далее – СОГ), состав которой определяется исходя из категории и вида совершенного преступления, в соответствии с требованиями нормативных правовых актов МВД России, регламентирующих деятельность дежурных частей органа внутренних дел, обеспечивает выезжающих сотрудников средствами связи, криминалистической техникой и транспортом для доставления к месту происшествия и обратно.

3. Докладывает начальнику органа внутренних дел или ответственному от руководящего состава органа внутренних дел с последующим информированием их о результатах работы дежурной СОГ о совершении дистанционного хищения и принятых мерах незамедлительно и организует выполнение полученных указаний.

¹¹ Разработанные Московским уголовным розыском ГУ МВД России по г. Москве методические рекомендации и алгоритм от 11 сентября 2024 г. № 1/8415.

4. Поддерживает связь с дежурной СОГ для постоянного получения объективной информации по оперативной обстановке с целью принятия дополнительных мер по организации работы на месте происшествия.

5. Передает в случае подтверждения информации о преступлении в дежурную часть вышестоящего органа внутренних дел и докладывает о результатах проведенных следственных действий и оперативно-розыскных мероприятиях.

При формировании оперативной сводки (информации) необходимо обращать внимание на способ совершения преступления¹²:

– **мошенничество (кража) в сети Интернет (интернет-магазины, электронные площадки по продаже товара, «ВКонтакте», «Одноклассники» и т. д.).** При заполнении информации о данном виде преступления в обязательном порядке вносит в оперативную сводку следующие сведения (при наличии таковых): абонентские номера телефонов потерпевшего и преступника; номер счета (карты) потерпевшего и преступника; электронный адрес сайта преступника, на котором размещаются сведения о продаже товара (ссылка на электронное объявление «Из Рук в Руки», «Авито» и т. д.); адрес электронной почты преступника, с помощью которой осуществлялась переписка; сведения о преступнике, которыми располагает потерпевший;

– **мошенничество, совершенное в современном информационном пространстве с использованием средств сотовой связи (когда потерпевший не предоставлял преступнику данные о своей банковской карте, пароли и т. д.).** При заполнении информации о данном виде преступления в обязательном порядке вносит в оперативную сводку следующие сведения (при наличии таковых): абонентские номера телефонов потерпевшего и преступника; номер счета (карты) потерпевшего и преступника; номер IMEI-устройства потерпевшего; сведения о преступнике, которые он сообщил потерпевшему; содержание СМС-сообщений, поступивших потерпевшему от преступника;

– **кража, совершенная с использованием средств сотовой связи (когда потерпевший лично предоставил преступнику данные о своей банковской карте, пароли из СМС-сообщений, CVV-код и т. д.).** При заполнении информации о данном виде преступления в обязательном порядке вносит в оперативную сводку следующие сведения (при наличии таковых): абонентские номера телефонов потерпевшего и преступника;

¹² Инструкция по заполнению оперативных сводок по преступлениям, совершенным дистанционным способом, в т. ч. преступлений, ответственность за которые предусмотрена пунктом «г» ч. 3 ст. 158 УК РФ от 19 августа 2019 г. № 10/1366.

номер счета (карты) потерпевшего и преступника; номер IMEI-устройства потерпевшего; сведения о преступнике, которыми располагает потерпевший; содержание СМС-сообщений, поступивших потерпевшему от преступника.

Также должностному лицу, формирующему оперативную сводку, в обязательном порядке необходимо вносить в фабулу слова-маркеры:

– **по кражам (ст. 158 УК РФ):**

- с банковской карты;
- с банковской карты – с похищенного телефона;
- с банковской карты – покупка (продажа) через интернет;
- с банковской карты – социальная служба (медицина);
- с банковской карты – сотрудник банка;

– **по мошенничествам (ст. 159 УК РФ):**

- с банковской картой;
- попал в беду;
- медицина;
- социальная служба;
- социальные сети;
- сайт с частным объявлением.

2.2. Действия следователей (дознавателей) в процессе расследования уголовных дел до полного выяснения всех обстоятельств и установления лиц, причастных к совершению преступлений в современном информационном пространстве с использованием сети Интернет¹³

При квалификации данных действий следует руководствоваться разъяснениями, содержащимися в постановлениях Пленума Верховного Суда Российской Федерации: от 27 декабря 2002 г. № 29 (ред. от 15 декабря 2022 г.) «О судебной практике по делам о краже, грабеже и разбое»¹⁴

¹³Методические рекомендации по расследованию преступлений, совершенных дистанционным способом, разработанные ГУ МВД России по г. Москве от 15 августа 2019 г. № 38/15789.

¹⁴ О судебной практике по делам о краже, грабеже и разбое: постановление Пленума Верховного Суда Российской Федерации: от 27 декабря 2002 г. № 29 (ред. от 15 декабря 2022 г.) // СПС «КонсультантПлюс»: [сайт]. URL: https://www.consultant.ru/document/cons_doc_LAW_40412/ (дата обращения: 10.12.2025).

и от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате»¹⁵.

К основным (наиболее распространенным) преступлениям указанной категории относятся составы преступлений, предусмотренные п. «г» ч. 3 ст. 158, ст. 159³, 159⁶ УК РФ.

Федеральным законом от 23 апреля 2018 г. № 111-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации»¹⁶ наименование ст. 159³ УК РФ и диспозиция ч. 1 изложены в новой редакции: «Статья 159³ Мошенничество с использованием электронных средств платежа». Указанные изменения вступили в силу с 4 мая 2018 г. Ранее статья 159³ УК РФ называлась «Мошенничество с использованием платежных карт», а диспозиция ч. 1 была сформулирована следующим образом: «Мошенничество с использованием платежных карт, то есть хищение чужого имущества, совершенное с использованием поддельной или принадлежащей другому лицу кредитной, расчетной или иной платежной карты путем обмана уполномоченного работника кредитной, торговой или иной организации». Одновременно была усилена и уголовная ответственность за преступления, предусмотренные ч. 1 ст. 159.3 УК РФ, – наказание в виде ареста на срок до четырех месяцев заменено на лишение свободы на срок до трех лет.

Кроме того, в результате исключения указания на ст. 159³ УК РФ из примечания к ст. 159¹ УК РФ и из п. 4 примечания к ст. 158 УК РФ снижено значение крупного размера с 1,5 млн руб. до 250 тыс. руб., особо крупного – с 6 млн руб. до 1 млн руб. Крупный и особо крупный размер в ст. 159³ определяется исходя из положений п. 4 примечания к ст. 158 УК РФ.

В то же время указанным Федеральным законом внесены изменения в ч. 3 ст. 158 УК РФ, которая дополнена п. «г» в следующей редакции: «Кража, совершенная с банковского счета, а равно в отношении электронных денежных средств (при отсутствии признаков преступления, предусмотренного ст. 159³ настоящего Кодекса)», санкция за совершение которой предусматривает лишение свободы на срок до 6 лет.

¹⁵ О судебной практике по делам о мошенничестве, присвоении и растрате: постановление Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48 (ред. от 15 декабря 2022 г.) // СПС «КонсультантПлюс»: [сайт]. URL: https://www.consultant.ru/document/cons_doc_LAW_283918/ (дата обращения: 25.12.2025).

¹⁶ О внесении изменений в Уголовный кодекс Российской Федерации: Федеральный закон от 23 апреля 2018 г. № 111-ФЗ // СПС «КонсультантПлюс»: [сайт]. URL: https://www.consultant.ru/document/cons_doc_LAW_296451/ (дата обращения: 10.12.2025).

Кроме того, преступление, предусмотренное п. «г» ч. 3 ст. 158 УК РФ, может совершаться с использованием системы «Мобильный банк» уже после совершения преступления, связанного с незаконным завладением мобильным телефоном, то есть совершение преступления небольшой и средней тяжести (хищение телефона) влечет совершение тяжкого преступления и, соответственно, образует два самостоятельных состава преступления.

При поступлении информации о завладении (хищении) мобильным телефоном необходимо обеспечить проверку информации о подключении системы «Мобильный банк», в том числе с целью ее незамедлительного отключения.

С целью обеспечения возможности качественного проведения анализа совершенных преступлений, для заполнения документов первичного учета установлены кодовые значения способа совершения преступлений, совершенных дистанционным способом, по которым вносится информация в модуль «Уголовное дело» сервиса обеспечения деятельности дежурных частей Единой системы информационно-аналитического обеспечения деятельности МВД России (СОДЧ ИСОД МВД России):

- 49 (с использованием средств мобильной связи);
- 771 (в т. ч. под предлогом освобождения от уголовной ответственности);
- 772 (в т. ч. получение компенсации за ранее приобретенные БАДы);
- 773 (в т. ч. получение выигрыша в различных лотереях);
- 774 (в т. ч. разблокирование банковской карты);
- 775 (в т. ч. осуществление оккультных услуг);
- 781 (в т. ч. пополнение счета);
- 784 (под предлогом продажи товаров через Интернет).

Действия виновных лиц квалифицируются по ст. 159 УК РФ, если они связаны с введением владельца денежных средств или иного имущества в заблуждение или с использованием доверительных отношений с ним, в результате чего тот передал денежные средства, иное имущество (право на имущество) – осуществил отчуждение имеющихся у него безналичных денежных средств путем перевода на указанный расчетный счет (банковскую карту, электронный кошелек, номер мобильного телефона и пр.).

Примером совершения такого мошенничества является введение в заблуждение лица или использование доверительных отношений с ним в ходе телефонного разговора (в том числе рассылка сообщений на мобильные средства связи, электронных писем и пр.) путем сообщения заведомо ложной, недостоверной информации, основываясь на которой заявитель действует в интересах виновного.

Под различными вымышленными предложениями достаточно часто сообщается заведомо ложная информация: о необходимости разблокирования банковской карты, для чего следует совершить ряд действий с мобильным средством связи; предоставленной компенсации за ранее приобретенные медицинские препараты; перечислениях от Пенсионного фонда, для чего необходимо сообщить реквизиты банковской карты; необходимости перевода денежных средств за решение возникших проблем у родственника, который попал в ДТП, совершил преступление; направляется электронное письмо (сообщение) о взломе (блокировке) страницы в социальной сети, для разблокировки которой необходимо перевести определенную сумму денег.

Действия лица следует квалифицировать по ст. 159³ УК РФ в случаях, когда хищение имущества осуществлялось с использованием поддельной или принадлежащей другому лицу кредитной, расчетной или иной платежной карты путем сообщения уполномоченному работнику кредитной, торговой или иной организации заведомо ложных сведений о принадлежности указанному лицу такой карты на законных основаниях либо путем умолчания о незаконном владении им платежной картой.

Хищение чужих денежных средств, находящихся на счетах в банках путем использования похищенной или поддельной кредитной либо расчетной карты следует квалифицировать как мошенничество только в тех случаях, когда лицо путем обмана или злоупотребления доверием ввело в заблуждение уполномоченного работника кредитной, торговой или сервисной организации (например, в случаях, когда, используя банковскую карту для оплаты товаров или услуг в торговом или сервисном центре, лицо ставит подпись в чеке на покупку вместо законного владельца карты либо предъявляет поддельный паспорт на его имя). Аналогичным образом должно квалифицироваться и использование похищенной либо поддельной платежной карты для оплаты товаров или услуг, даже если от виновного лица не потребовалось вводить ПИН-код карты¹⁷, предъявлять паспорт или расписываться вместо законного владельца карты.

Согласно п. 21 постановления Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве,

¹⁷ ПИН-код (англ. PIN *personal identification number*) – персональный идентификационный номер, являющийся секретным кодом карты, при этом на ней он не хранится. Его длина варьирует от 4 до 12 цифр, на практике чаще всего встречается из 4. ПИН-код может состоять также из букв. Он вводится с помощью специального криптографического модуля, входящего в состав терминального устройства (банкомата, POS-терминала и т.п.) и передается в адрес эмитента, где он проверяется. Знание ПИН-кода, известного только держателю карты, по которой производится транзакция, является основанием считать, что лицо, совершающее операцию, и держатель карты являются одним лицом.

присвоении и растрате», «в тех случаях, когда хищение совершается путем использования учетных данных собственника или иного владельца имущества независимо от способа получения доступа к таким данным (тайно либо путем обмана воспользовался телефоном потерпевшего, подключенным к услуге «Мобильный банк», авторизовался в системе интернет-платежей под известными ему данными другого лица и т. п.), такие действия подлежат квалификации как *кража*, если виновным не было оказано незаконного воздействия на программное обеспечение серверов, компьютеров или на сами информационно-телекоммуникационные сети». Другими словами, если лицо похитило безналичные денежные средства, воспользовавшись необходимой для получения доступа к ним конфиденциальной информацией держателя платежной карты (например, персональными данными владельца, его платежной карты, контрольной информацией, паролями), переданной самим держателем платежной карты под воздействием обмана или злоупотребления доверием.

В случае, когда неправомерное завладение чужим имуществом (денежными средствами) или приобретение права на имущество осуществлялись без ведома и помимо воли законного владельца путем неправомерного вмешательства в функционирование компьютерных устройств или информационно-телекоммуникационных сетей, путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей, такие действия необходимо квалифицировать по ст. 159⁶ УК РФ.

Под *неправомерным вмешательством* необходимо понимать целенаправленное воздействие программных и (или) программно-аппаратных средств на серверы, средства вычислительной техники (компьютеры), в том числе переносные (портативные) – ноутбуки, планшетные компьютеры, смартфоны, снабженные соответствующим программным обеспечением, или на информационно-телекоммуникационные сети, которое нарушает установленный процесс обработки, хранения, передачи компьютерной информации, что позволяет виновному или иному лицу незаконно завладеть чужим имуществом или приобрести право на него.

Типичным примером мошенничества в сфере компьютерной информации (ст. 159⁶ УК РФ) является получение путем обмана или иным незаконным способом, в частности в современном информационном пространстве с помощью распространения по сети Интернет, вредоносных компьютерных программ, кодов доступа к банковским счетам и последующий перевод находящихся на этих счетах денежных средств.

Некоторые действия по незаконному переводу денежных средств посредством воздействия на компьютерную информацию, совершаемые без ведома и помимо воли потерпевшего, в правоприменительной практике органов дознания и предварительного следствия нередко квалифицируются как кража по ст. 158 УК РФ. Однако судами подобные действия квалифицируются в основном как мошенничество в сфере компьютерной информации, и действия виновных зачастую переквалифицируются на ст. 159⁶ УК РФ, что следует признать правильным.

К данному виду мошенничеств можно отнести распространение вредоносного программного обеспечения, которое блокирует компьютер или делает его использование невозможным (экран или часть экрана закрыта заставкой, либо по экрану хаотично двигается заставка, мешающая просмотру информации на экране монитора, либо на весь экран изображено требование отправить смс-сообщение на короткий номер для разблокирования компьютера); сообщение в виде электронного письма с вложенной (прикрепленной к электронному письму) ссылкой, переход по которой перенаправляет пользователя на определенный интернет-ресурс (страницу), где имеется предложение заведомо несуществующей услуги или методики (генератора электронных денег, пополнения так называемых кошельков с электронными деньгами, ставки на спорт) и пр.

Вышеописанные действия квалифицируются по ст. 159, 159³ и 159⁶ УК РФ, если общая стоимость похищенного имущества выше, чем размер мелкого хищения.

В соответствии со ст. 7.27 Кодекса Российской Федерации об административных правонарушениях¹⁸ (далее – КоАП РФ) размер мелкого хищения составляет в настоящее время не более 2 500 руб. В соответствии с примечанием 2 к ст. 158 УК РФ значительный ущерб гражданину в статьях УК РФ, предусматривающих ответственность за преступления против собственности, за исключением ч. 5 ст. 159 УК РФ, определяется с учетом его имущественного положения, но не может составлять менее 5 000 руб.

Мошеннические действия, причинившие ущерб на общую сумму менее 2 500 руб., квалифицируются по ст. 7.27 КоАП РФ как мелкое хищение, а в случаях их совершения лицом, подвергнутым административному наказанию за мелкое хищение, – по ст. 158¹ УК РФ. В то же время мошенничество в сфере компьютерной информации,

¹⁸ Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ. (ред. от 23.03.2026) (с изм. и доп., вступ. в силу с 03.04.2026) // СПС «КонсультантПлюс»: [сайт]. – URL: https://www.consultant.ru/document/cons_doc_LAW_34661/ (дата обращения: 10.04.2026).

совершенное посредством неправомерного доступа к компьютерной информации или посредством создания, использования и распространения вредоносных компьютерных программ, требует дополнительной квалификации по ст. 272, 273 или 274.1 УК РФ.

Мошеннические действия, совершенные группой лиц по предварительному сговору, лицом с использованием своего служебного положения, организованной группой, квалифицируются по соответствующим частям ст. 159–159.3, 159.5, 159.6 УК РФ независимо от размера причиненного ущерба, в том числе в случаях, когда он не превышает размера мелкого хищения.

Не образует состава мошенничества хищение чужих денежных средств путем использования заранее похищенной или поддельной платежной карты, если выдача наличных денежных средств была произведена посредством банкомата, без участия уполномоченного работника кредитной организации. В этом случае содеянное следует квалифицировать как кражу.

В тех случаях, когда хищение совершается путем использования учетных данных собственника или иного владельца имущества независимо от способа получения доступа к таким данным (лицо тайно либо путем обмана воспользовалось не принадлежащим ему телефоном, подключенным к услуге «Мобильный банк», авторизовалось в системе интернет-платежей под известными ему данными другого лица и т. п.), такие действия подлежат квалификации как кража, если виновным не было оказано незаконного воздействия на программное обеспечение серверов, компьютеров или на сами информационно-телекоммуникационные сети. При этом изменение данных о состоянии банковского счета и (или) о движении денежных средств, произошедшее в результате использования лицом не принадлежащих ему учетных данных, не может признаваться таким воздействием.

Если хищение чужого имущества или приобретение права на имущество осуществляются путем распространения заведомо ложных сведений в информационно-телекоммуникационных сетях, включая сеть Интернет, например создание поддельных сайтов благотворительных организаций, интернет-магазинов, электронной почты, то такое мошенничество квалифицируется по ст. 159, а не по ст. 159⁶ УК РФ (п. 21 постановления Пленума от 30 ноября 2017 г. № 48).

Также следует учесть, что на практике часто возникает вопрос о субъектах, которым причиняется ущерб в результате хищения денежных средств с использованием платежных карт. Данный вопрос должен решаться в зависимости от способа, посредством которого произошло мошенническое завладение денежными средствами. Если у лица похищена

платежная карта, карта утеряна, а затем похищены денежные средства с его счета, то потерпевшим признается указанное лицо. В случаях, когда для мошеннического завладения денежными средствами используется поддельная платежная карта в качестве потерпевшего признается банк-эквайер¹⁹. В подобной ситуации держателю карты ущерб не причиняется, так как банк-эмитент²⁰ должен возместить ему ущерб, причиненный в результате неправомерного расходования денежных средств на приобретение товаров, услуг через торговые или сервисные предприятия. Для возмещения причиненного ущерба держатель обязан сообщить об утрате им карты или необоснованных списаниях средств с его счета, что предусмотрено как действующим законодательством²¹, так и соответствующим договором между банком и клиентом.

Поскольку комплексное законодательное регулирование технологии функционирования платежных карт отсутствует, оно регулируется отдельными договорами, в том числе между эквайером и торгово-сервисными предприятиями (договор об эквайринге).

Необходимо обратить внимание на то, что в случаях, когда лицо с целью завладения банковской картой и дальнейшего ее использования применяет в отношении ее владельца насилие, не опасное для жизни и здоровья, квалификация действий по п. «г» ч. 2 ст. 161 УК РФ неверна, поскольку платежная карта не представляет материальной ценности и не обладает свойствами имущества, в связи с чем не содержит признаков предмета хищения. В таком случае применение насилия следует квалифицировать по ст. 116 УК РФ, а завладение картой, в зависимости от направленности умысла и иных обстоятельств дела, как приготовление (с учетом требований ч. 2 ст. 30 УК РФ) к мошенничеству либо краже.

Согласно п. 6 постановления Пленума Верховного Суда РФ от 27 декабря 2002 г. № 29, кража и грабеж считаются оконченными, если имущество изъято и виновный имеет реальную возможность им пользоваться или распоряжаться по своему усмотрению. В рассмотренных выше случаях изъятия имущества не происходит, поскольку денежные средства (предмет хищения) продолжают находиться

¹⁹ *Банк-эквайер* – банк или финансовое учреждение, которое обрабатывает платежи по кредитным или дебетовым картам от имени продавца.

²⁰ *Банк-эмитент* (лат. *emittere* – «выпускать, издавать») – финансово-кредитная организация, которая выпускает денежные знаки, платёжные средства (банковские карты) и ценные бумаги, а также исполняет обязательства по ним перед держателями. Также такой банк может называться эмиссионным.

²¹ О национальной платежной системе: Федеральный закон от 27 июня 2011 г. № 161-ФЗ (ст. 9) // СПС «КонсультантПлюс»: [сайт]. – URL: https://www.consultant.ru/document/cons_doc_LAW_115625/ (дата обращения: 20.12.2025).

на счете карты, выбывшей из распоряжения владельца. Само же изъятие имущества происходит скрытно, а преступник, например при снятии денежных средств со счета похищенной карты, осознает, что действует тайно и противоправность его действий не очевидна для окружающих.

В случае же, когда к лицу с целью завладения платежной картой применяется опасное для жизни или здоровья насилие либо угроза его применения, действия виновного должны квалифицироваться как разбой, поскольку данное преступление считается оконченным с момента нападения в целях хищения, вне зависимости от того, удалось ли преступнику фактически завладеть похищаемым имуществом, т. е. денежными средствами, находящимися на счете платежной карты.

Главным следственным управлением ГУ МВД России по г. Москве с учетом обобщения сведений правоприменительной практики органов предварительного расследования системы МВД России в иных субъектах Российской Федерации по уголовным делам по преступлениям, совершенным дистанционным способом, проведен анализ, который показал отсутствие единого подхода по установлению места совершения данной категории преступлений.

Так, согласно разъяснениям Генеральной прокуратуры Российской Федерации (исх. № 22-17-2018/Ип 12666-18 от 23 октября 2018 г.), направленным в адрес прокурора Пензенской области, следует, что местом совершения мошенничества, предметом которого являются безналичные денежные средства, признается место совершения деяния, содержащего признаки преступления, где оно было пресечено или окончено. В соответствии с п. 5 постановления Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48, если предметом преступления при мошенничестве являются безналичные денежные средства, то преступление считается оконченным с момента изъятия денежных средств с банковского счета их владельца или электронных денежных средств, в результате чего владельцу этих денежных средств причинен ущерб.

Данный подход вытекает из правовой природы безналичных денежных средств, которые в соответствии со ст. 128 Гражданского кодекса Российской Федерации от 30 ноября 1994 г. № 51-ФЗ²² как объекты гражданских прав наряду с бездокументарными ценными бумагами и имущественными правами относятся не к вещам, а к иному имуществу. В силу п. 1 и 2 ст. 845 ГК РФ денежные средства, переданные владельцем счета обслуживающему банку для зачисления их на свой банковский счет

²²Гражданский кодекс Российской Федерации от 30 ноября 1994 г. № 51-ФЗ // СПС «КонсультантПлюс»: [сайт]. – URL: https://www.consultant.ru/document/cons_doc_LAW_5142/ (дата обращения: 20.12.2025).

или поступившие на указанный счет от третьих лиц, становятся собственностью банка. При этом у банка возникает обязательство по поводу совершения операций по счету на основании распоряжения владельца счета.

Общее правило, определяющее момент окончания хищения, в том числе с изъятием наличных денег, связано с установлением реальной возможности виновного пользоваться или распоряжаться похищенным по своему усмотрению.

При хищении же безналичных денежных средств ситуация принципиально иная: определяющее значение имеет место, где были совершены общественно опасные действия (место нахождения банка, в котором незаконно изъяты со счета безналичные денежные средства), а не место наступления общественно опасного последствия в виде поступления денежных средств на счет виновного.

В части определения места совершения преступления по п. «г» ч. 3 ст. 158 УК РФ необходимо руководствоваться постановлением Пленума Верховного Суда Российской Федерации от 27 декабря 2002 г. № 29. Местом совершения преступления будет являться место завладения денежными средствами потерпевшего, а не адрес банка, где открыт счет потерпевшего и откуда списаны денежные средства.

Учитывая изложенное, следователь при производстве предварительного расследования по уголовным делам, возбужденным по преступлениям, совершенным дистанционным способом, должен документально устанавливать: полное наименование, адресные данные, реквизиты кредитно-финансовой организации и номер счета потерпевшего (с которого произошло хищение денежных средств), аналогичные информационные сведения в отношении расчетного счета, на который подозреваемым (обвиняемым) перечислены указанные средства потерпевшего, а равно, где лицо фактически завладело денежными средствами посредством банкомата (платежного терминала). Истребованная информация учитывается при составлении и предъявлении обвинения в порядке, предусмотренном ст. 171–175 Уголовно-процессуального кодекса Российской Федерации от 18 декабря 2001 г. № 174-ФЗ²³.

Также разработан общий алгоритм действий следователя после возбуждения уголовного дела по рассматриваемым категориям преступлений, при использовании которого следует учитывать, что совершаются данные преступления в различных сферах

²³ Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ (ред. от 08.03.2026) // СПС «КонсультантПлюс»: [сайт]. – URL: https://www.consultant.ru/document/cons_doc_LAW_34481/ (дата обращения: 20.03.2026).

жизнедеятельности, при различных обстоятельствах, в связи с чем требуют индивидуализации в своем применении.

Так, следователю после возбуждения уголовного дела рекомендуется провести ряд следственных и процессуальных действий, направленных на раскрытие рассматриваемой категории преступлений, в том числе:

– составить план следственных действий и оперативно-розыскных мероприятий, в который необходимо включить версии, подлежащие проверке, следственные действия и оперативно-розыскные мероприятия со сроками их выполнения и указанием в обязательном порядке исполнителя;

– признать потерпевшим лицо, которому причинен материальный ущерб, допросив его по следующим вопросам:

- дата, время поступления звонка (СМС-сообщения) с соответствующим содержанием;

- абонентский номер потерпевшего, на который был осуществлен звонок (стационарный, мобильный телефон), если имеется автоматический определитель номера, указать, с какого номера телефона осуществлен звонок;

- дословное содержание разговора, кем представился звонивший, о чем говорил, что предлагал сделать (содержание СМС-сообщений);

- описание голоса звонившего: дефекты и особенности речи – хрипота, картавость, шепелявость, заикание; интонация голоса, разговаривал ли он шепотом или обычным тембром; какие особенности, странности в интонации, произношении звуков, в обращении заметил потерпевший; использование в разговоре специальных терминов, специфических речевых оборотов; по каким приметам потерпевший сможет опознать его голос;

- качество связи (помехи, слышимость, разговор прерывался);

- что именно (по возможности дословно) сам потерпевший сообщил неизвестному, представившемуся родственником (сотрудникам банка, полиции, иной организации);

- как неизвестный узнал точный адрес места жительства потерпевшего: последний сам назвал его либо неизвестный, представившийся одним из указанных выше лиц, уже знал его место жительства;

- как долго по времени длился телефонный разговор с неизвестным (сверить в последующем с данными детализации телефонных переговоров);

- через какой период времени после окончания разговора подъехал звонивший неизвестный к дому потерпевшего;

- описание голоса неизвестного лица (курьера, таксиста), какие особенности, странности в интонации, произношении звуков, в обращении к нему заметил, по каким приметам сможет опознать его голос;

- подробное описание черт его лица, рук, особенностей телосложения, походки, поведения, по которым потерпевший сможет его опознать (составить композиционный портрет личности), одежды;

- если передача денег осуществлялась в жилище потерпевшего, установить: когда неизвестный курьер (таксист) зашел в квартиру, то до каких предметов мебели, иных предметов дотрагивался, как себя вел, что сообщил, задавал ли какие-либо вопросы;

- сообщал ли потерпевший 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 (банковской карты), а также пересчитывал ли потерпевший или неизвестное лицо на месте передачи деньги;

- звонил ли неизвестный в момент получения денег кому-либо, что говорил;

- провожал ли потерпевший неизвестного, наблюдал ли за направлением, в котором неизвестный покинул место расположения его дома, передвигался ли неизвестный на автомобиле (какой модели);

- кто из посторонних лиц посещает или посещал в последнее время потерпевшего (социальный работник, медицинский работник, представитель организации по вопросам пенсионного обеспечения и пр.), его полные анкетные данные, контактные номера телефонов, как может охарактеризовать его, когда последний раз тот его посещал;

- 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 потерпевшим действия после обнаружения факта мошеннических действий (хищение денежных средств с карты);

- является ли ущерб значительным для потерпевшего, если да, то обязательно отразить обстоятельства, подтверждающие это, каков состав семьи, близких родственников, лиц, находящихся на иждивении, размер доходов и расходов заявителя по состоянию на момент совершения в отношении него преступления.

При допросе потерпевшего по уголовному делу о дистанционном мошенничестве, совершенном с использованием информационно-телекоммуникационной сети Интернет, необходимо выяснить:

- дату и время обнаружения объявления (получения ссылки на соответствующий интернет-ресурс), сохранились ли данные объявления (№ объявления, страницы), если возможно – найти объявление в интернете и зафиксировать его адрес (еще раз пройти по интернет-ссылке), сделать снимок экрана, приобщить его к материалам дела;

- с использованием какого технического устройства потерпевший выходил на сайт с размещенным объявлением (переходил по интернет-ссылке) – стационарного компьютера, мобильного устройства;

- 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;

- каким образом, когда (дата, время) заявитель связался с продавцом, как он представился, указывал ли свое местоположение;

- известно ли ему место нахождения товара;

- подробное содержание разговора с продавцом;

- что именно сообщил продавец о продаваемом товаре, об условиях оплаты товара, условиях, сроках и способах доставки покупателю товара;

- описание голоса продавца, сможет ли опознать (по каким приметам);

- когда (дата, период времени), каким образом (через банкомат, посредством услуги «Сбербанк Онлайн», «Мобильный банк»), в каком размере и на какой счет (№ счета либо банковской карты, на чье имя открыты) потерпевший перечислил денежные средства в счет оплаты за якобы приобретаемый товар;

- если потерпевший осуществил перевод денежных средств со своей банковской карты на банковскую карту неизвестного посредством услуги «Сбербанк Онлайн», через «Личный кабинет», установить место входа

потерпевшего в сеть Интернет (с какого компьютера, ноутбука, планшета, с использованием какого модема, роутера, их MAC-адреса, логины и пароли, какая компания-провайдер предоставляла в этот день заявителю услуги доступа в интернет);

- дату и место открытия счета (банковской карты), с которой потерпевший перечислил денежные средства;

- каким образом известил «продавца товара» о перечислении денежных средств на указанную им банковскую карту (электронный кошелек);

- что именно ему сообщил после подтверждения оплаты (перечисления денег на банковскую карту виновного) «продавец»;

- в какой период времени, куда прибыл для получения (как ему казалось) приобретенного товара;

- когда он осознал, что в отношении него было совершено мошенничество, в результате которого похищены принадлежащие ему денежные средства;

- предпринятые потерпевшим действия после обнаружения факта мошеннических действий.

При допросе потерпевшего по уголовному делу о дистанционном мошенничестве, совершенном с использованием вредоносного программного обеспечения, необходимо выяснить:

- время, место и обстоятельства хищения денежных средств;

- реквизиты банковской карты, с которой совершено хищение денежных средств, а также подключенной услуги «Мобильный банк» с указанием номеров телефонов, к которым она привязана;

- если услуга подключена самим потерпевшим, то с какого времени и каким способом (посредством заявления о подключении в офисах банковских учреждений или посредством банкоматов);

- с какого времени потерпевший пользуется абонентским номером, к которому данная услуга подключена, т. к. не исключается перевыпуск номера оператором сотовой связи по истечении 6 месяцев неиспользования абонентского номера с оформлением номера на иное лицо;

- модель телефона, подключенного к услуге «Мобильный банк», используемая операционная система в телефоне («Андроид», «IOS» (Apple) или иное), наличие в нём установленных антивирусных программ;

- какие мобильные приложения устанавливались в последнее время, способ установки (из официальных источников (сайтов) «Андроид», «IOS» (Apple), с сайта банка-имитента банковской карты (банковского продукта, в случае, например, открытия банковского счета без выпуска банковской карты);

– совершались ли операции через мобильное устройство (телефон, планшет) или компьютер, вводились ли иным способом данные карты или хранились сведения о ней в устройствах;

– осуществлялся ли с данного устройства доступ в сеть Интернет, в том числе автоматически, например при установке графика автоматического обновления приложений; если да, то каких именно приложений;

– осуществлял ли кто-либо с использованием данных банковской карты (номера, срока действия, данных владельца, CVC/CVV2-кода (три цифры, расположенные на обратной стороне банковской карты) потерпевшего покупку товаров, заказ услуг через сеть Интернет;

– поступали ли на мобильное устройство сообщения, содержащие ссылки на интернет-ресурсы, если да, то, когда, от кого, содержание сообщений, осуществлялся ли переход по данным ссылкам, если да, то каков результат (было установлено приложение, установка приложения неожиданно прервалась, мобильное устройство «зависло», потребовалась перезагрузка, приложение «попросило» ввести определенные данные и пр.);

– ремонтировалось ли устройство до или после обнаружения факта хищения, где и кем;

– поступали ли сообщения о снятии денежных средств, их содержание, номер, с которого они были отправлены;

– местонахождение мобильного телефона в настоящее время, а также желает ли потерпевший добровольно предоставить его для производства компьютерной экспертизы с указанием необходимых паролей;

– обращался ли потерпевший в банк, имеются ли у него выписки о движении денежных средств по карте, ответы по обращениям (в случае наличия таковых приобщить их к материалам проводимой проверки).

При допросе потерпевшего по уголовному делу о мошенничестве (краже), совершенном с использованием похищенной или поддельной кредитной либо расчетной карты, необходимо выяснить:

– кто имел доступ к карте или знал ПИН-код;

– какими кредитными, торговыми, сервисными или иными организациями, банкоматами пользовался, какие расчетно-платежные операции проводил, кто при этом присутствовал;

– производил ли оплату товаров, работ, услуг через сеть Интернет, какими сайтами пользовался;

– получал ли смс-сообщения о предоставлении продуктов и услуг банка с предложением нажать определенные клавиши на телефоне для подтверждения согласия в их приобретении или смс-сообщения о блокировке карты с номером телефона, по которому необходимо

перезвонить, какие сведения в таких ситуациях он передавал, сообщал ли персональные данные платежных карт, какие именно;

- имело ли место поступление на электронную почту сообщений от кредитных организаций, их содержание, перечень сведений, переданных им по просьбе банков;

- время последнего использования карты, месторасположение сервисного предприятия или банкомата, где карта применялась в последний раз, перечень полученных услуг или приобретенных товаров (предметов);

- обстоятельства утраты или похищения карты, если это имело место (или производится изъятие платежной карты и ее осмотр, если карта находится у потерпевшего), истребовать и проверить подлинность и действительность документов, подтверждающих материальный ущерб, причиненный потерпевшему в результате хищения денежных средств;

а также:

- разъяснить потерпевшему право на заявление гражданского иска на сумму причиненного ущерба в рамках расследования уголовного дела;

- в случае написания искового заявления, в соответствии со ст. 44 Уголовно-процессуального кодекса РФ²⁴ (далее – УПК РФ), признать его гражданским истцом по уголовному делу;

- произвести (при необходимости) выемку имеющих значение для уголовного дела предметов и документов, находящихся у потерпевшего; направить потерпевшего на составление композиционного портрета (если имел место быть прямой контакт), предъявление фотокартотеки лиц, ранее судимых и состоящих на учете в ОМВД, в случае, если указанные мероприятия не были выполнены в рамках доследственной проверки;

- направить ориентировки в территориальные ОМВД г. Москвы с приметами подозреваемого (если имел место быть прямой контакт), в случае невыполнения указанных мероприятий в рамках доследственной проверки;

- допросить в качестве свидетелей лиц, на которых указывает потерпевший или в отношении которых имеются достаточные сведения как о возможных свидетелях происшедшего, в том числе и родственников потерпевшего, при необходимости направить их на составление композиционного портрета, предъявление фотокартотеки лиц, ранее судимых и состоящих на учете в органах внутренних дел;

²⁴ Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ (ред. от 8 марта 2026 г.) // СПС «КонсультантПлюс»: [сайт]. – URL: https://www.consultant.ru/document/cons_doc_LAW_34481/ (дата обращения: 15.03.2026).

– направить в порядке ст. 38 УПК РФ поручение в оперативные службы ОМВД об установлении лиц, причастных к совершению преступления, отработке на причастность к совершенному преступлению лиц, ранее судимых за аналогичные преступления; в порядке ст. 186.1 УПК РФ обратиться в суд с ходатайством об истребовании у оператора сотовой связи входящих и исходящих телефонных соединений абонентского номера, с которого звонили потерпевшему, с указанием места нахождения (адресов) базовых станций, а также информации, на чье имя зарегистрирован указанный абонентский номер;

– направить запросы в банковские учреждения для получения сведений:

- о номере счета, на который потерпевшими осуществлялись денежные переводы;

- лице, на чье имя (паспортные данные, адрес фактического проживания, контактные номера) зарегистрирован расчетный счет;

- подключении услуги «Мобильный банк», с указанием номеров телефонов и периода действия;

- подключении услуги «Сбербанк Онлайн» (или аналогичной услуги в других кредитных учреждениях), дате подключения и способе получения паролей;

- других подключенных услугах по смс-подтверждению операций, с указанием номеров телефонов и периода действия;

- снятии денежных средств в кредитных учреждениях и банкоматах;

– в случае использования мошенником для совершения преступления банковской карты направить запрос в банковские учреждения для установления и выявления сведений по карте, на которую потерпевший перевел денежные средства, а именно:

- о дате выпуска карты, когда и где она выпущена (номер и адрес офиса) и получена, номер лицевого счета; имеются ли у лицевого счета другие карты, если имеются, то указать их номера, период действия;

- держателе карты (паспортные данные, адрес фактического проживания, контактные номера);

- подключении услуги «Мобильный банк», с указанием номеров телефонов и периода действия;

- подключении услуги «Сбербанк Онлайн» (или аналогичной услуги в других кредитных учреждениях), дате подключения и способе получения паролей; других подключенных услугах по СМС-подтверждению операций, с указанием номеров телефонов и периода действия;

- производстве выемки видеозаписей момента снятия денежных средств преступником;

- изъятии видеозаписи с камер уличного видеонаблюдения, где непосредственно была осуществлена передача денежных средств, камер видеонаблюдения, установленных в банках, торговых центрах, банкоматах, где осуществлялся перевод или снятие денежных средств преступником;

- в случае, если денежные средства передавались через работников такси, получить в Единой диспетчерской службе сведения о том, кто из работников мог находиться в момент передачи денежных средств в указанном месте;

- в случае, если имеются сведения только о марке автомашины, путях отхода, направить запрос в АПК «Безопасный город» с целью установления государственного номера автомобиля, лица, которому были переданы денежные средства;

- в случае установления водителя автомашины (водителя такси), которому были переданы денежные средства:

- провести его опознание потерпевшим, отработать его личную заинтересованность;

- выяснить сумму вознаграждения за оказанные услуги;

- выяснить, через кого и как осуществляется связь между ним и преступником;

- направить его для составления композиционного портрета, если он передал денежные средства непосредственно преступнику;

- произвести выемку журналов регистрации вызовов;

- в случае установления лица, на чье имя зарегистрированы абонентский номер, расчетный счет, банковская карта, необходимо допросить его в качестве свидетеля; в случае, если указанное лицо проживает в другом регионе, направить поручение в оперативные службы ОМВД с целью отработки на причастность его к совершенному преступлению;

- в случае, если указанное лицо сообщает, что не оформляло на свое имя абонентский номер (расчетный счет, банковскую карту):

- получить разрешение суда и произвести выемку регистрационного дела абонентского номера (расчетного счета, банковской карты);

- провести почерковедческие судебные экспертизы;

- допросить в качестве свидетелей работников организаций об обстоятельствах регистрации (открытия) абонентского номера (расчетного счета, банковской карты);

- направить поручение в оперативные службы ОВД с целью отработки на причастность к совершенному преступлению работников организаций, где была осуществлена регистрация (открытие) абонентского номера (расчетного счета, банковской карты);

- направить поручение в оперативные службы ОМВД с целью наблюдения за «курьерами» (таксистами) для документирования фактов получения ими денег от потерпевших и передачи третьим лицам (или оставление в обусловленных местах);

- провести оперативно-технические мероприятия, в том числе прослушивание телефонных переговоров лиц, номера которых установлены после совершения первых эпизодов;

- получить образцы голосов установленных преступников для обеспечения проведения в дальнейшем фоноскопических экспертиз;

- провести опознание потерпевшими голосов обвиняемых;

- при наличии сведений от оператора, что телефон, с которого звонили потерпевшему, работал в расположении исправительных учреждений и следственных изоляторов, необходимо направить поручение в оперативные службы данных учреждений с целью установления лиц, причастных к совершению преступления;

- допросить в качестве свидетелей сотрудников ФСИН;

- в случае установления лица, причастного к совершению преступления, находящегося в исправительных учреждениях и следственных изоляторах:

- провести в камере совместно с сотрудниками ФСИН осмотр (обыск) для установления и изъятия сотовых телефонов, сим-карт, листов с записями (с целью обеспечения назначения в последующем экспертиз);

- допросить в качестве свидетелей лиц, отбывающих наказание совместно с мошенником;

- провести обыски по месту жительства виновных лиц, сообщников, месту нахождения офисов (организаций);

- осмотреть, признать и приобщить к уголовному делу в качестве вещественных доказательств изъятые в ходе расследования уголовного дела предметы, документы, видеозаписи;

- направить запросы на получение характеризующего материала на виновных лиц;

- принять меры к возмещению ущерба, в том числе направить запросы в кредитные учреждения, МРЭО ГИБДД, Росреестр и иные организации;

- в случае установления имущества, на которое возможно наложить арест, в порядке ст. 115 УПК РФ обратиться в суд с ходатайством о наложении ареста на указанное имущество;

- предъявить обвинение виновным лицам в соответствии со ст. 171–175 УПК РФ;

- выполнить требования ст. 215–217 УПК РФ.

2.3. Действия сотрудников оперативных подразделений при получении информации о преступлении, совершенном в современном информационном пространстве с использованием сети Интернет

2.3.1. Осуществляют мероприятия в соответствии с действующими нормативными правовыми актами МВД России по установлению, обнаружению и задержанию лиц, подозреваемых в совершении преступления.

2.3.2. По поручению оперативного дежурного принимают меры к сбору материала проверки, а именно – получают подробное объяснение от гражданина, в отношении которого совершены преступные действия, в котором обращают внимание на способ совершения преступления²⁵:

– *мошенничество (кража) в сети Интернет* (интернет-магазины, электронные площадки по продаже товара, «ВКонтакте», «Одноклассники» и т. д.): при получении объяснения должностному лицу в обязательном порядке необходимо указывать следующие сведения:

- абонентские номера телефонов потерпевшего и преступника;
- номер счета (карты) потерпевшего и преступника;
- электронный адрес сайта преступника, где размещаются сведения о продаже товара (ссылка на электронное объявление «Из Рук в Руки», «Авито», «ВКонтакте» и т. д.);
- адрес электронной почты преступника, с помощью которой осуществлялась переписка (если таковой имеется);
- сведения о преступнике, которые он сообщил потерпевшему;

– *мошенничество, совершенное с использованием средств сотовой связи* (когда потерпевший не предоставлял преступнику данные о своей банковской карте, пароли и т.д.): при получении объяснения должностному лицу в обязательном порядке необходимо указывать следующие сведения:

- абонентские номера телефонов потерпевшего и преступника;
- номер счета (карты) потерпевшего и преступника;
- номер IMEI-устройства потерпевшего;
- сведения о преступнике, которые он сообщил потерпевшему;
- содержание СМС-сообщений, поступивших потерпевшему от преступника (если таковые имеются);

²⁵ Разработанный ОУ ГУ МВД России по г. Москве алгоритм действий сотрудников УР при опросе потерпевших по фактам дистанционных хищений от 30 сентября 2019 г. № 3/20423.

– кража, совершенная с использованием средств сотовой связи (когда потерпевший лично предоставил преступнику данные о своей банковской карте, пароли из СМС-сообщений, CVV-код и т. д.): при получении объяснения должностному лицу в обязательном порядке необходимо указывать:

- абонентские номера телефонов потерпевшего и преступника;
- номер счета (карты) потерпевшего и преступника;
- номер IMEI-устройства потерпевшего;
- сведения о преступнике, которые он сообщил потерпевшему;
- содержание СМС-сообщений, поступивших потерпевшему от преступника (если таковые имеются).

2.3.3. Истребуют у заявителя и приобщают к материалу проверки:

– детализацию телефонных соединений за период его общения с подозреваемым;

– расширенную выписку о движении денежных средств по счету потерпевшего, а также сведения о наличии либо отсутствии подключенной услуги «Мобильный банк», с указанием абонентских номеров;

– все чеки, квитанции, интернет-переписку, выписки по банковскому счету, банковскую карту, со счета которой похищались денежные средства, скриншот переписки с мошенником, сохранившиеся у потерпевшего.

2.3.4. Устанавливают, куда перечислены денежные средства, месторасположение банка, кто и где снял денежные средства, на кого зарегистрирован счет, направляют соответствующий запрос в установленные кредитные организации.

2.3.5. Приобщают видеозаписи с камер уличного видеонаблюдения, где непосредственно была осуществлена передача денежных средств, камер видеонаблюдения, установленных в банках, торговых центрах, банкоматах и т. д., где осуществлялся перевод.

2.3.6. Сообщают в дежурную часть сведения об обстоятельствах совершенного преступления, приметах подозреваемых лиц, а также другие данные, имеющие доказательственное значение для дальнейшего внесения сведений в оперативную сводку и проведения качественного анализа.

2.3.7. Принимают процессуальное решение по материалу предварительной проверки в соответствии с приказом МВД России от 3 апреля 2018 г. № 196 «О некоторых мерах по совершенствованию организации раскрытия и расследования отдельных видов хищений»²⁶, если иное не предусмотрено действующим законодательством.

²⁶ О некоторых мерах по совершенствованию организации раскрытия и расследования отдельных видов хищений: приказ МВД России от 3 апреля 2018 г. № 196. – URL: <https://юфоут.мвд.рф/document/13608728> (дата обращения: 12.12.2025).

2.3.8. При получении поручения следователя (дознвателя) по уголовному делу о дистанционном мошенничестве **ЗАПРАШИВАЮТ СВЕДЕНИЯ:**

1. У сотовых операторов:

- паспортные данные владельца абонентского номера;
- детализацию звонков за последние три-шесть месяцев (эти сведения позволяют определить, сколько у мошенника сотовых аппаратов (IMEI), как часто он меняет абонентские номера, а также избавляется ли он от сим-карты после совершения мошеннических действий или же использует повторно;
- использованные для связи абонентские устройства (IMEI);
- использованные для связи базовые станции с указанием адреса расположения и технических характеристик;
- 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, зарегистрированные 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 сим-карты при ее регистрации. Помимо установочных данных мы узнаем данные об адресе торговой точки, где она была реализована, а также данные продавца.

2. По банковским картам и расчетным счетам:

По банковской карте:

- о паспортных данных владельца банковской карты;
- движении денежных средств по банковской карте и местах их обналичивания за последние полгода с указанием точного времени проведения приходных и расходных операций, номеров и кодов 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, где совершались покупки. Каждый интернет-магазин предоставит информацию об адресе мошенника, на который почтовым переводом был отправлен приобретенный товар;

- абонентских номерах, привязанных к данной банковской карте услугой «Мобильного банка», где и каким образом они были подключены;
- адресе офиса банка, в котором была открыта банковская карта;
- IP-адресах, использованных для входа в онлайн-сервис по управлению данной банковской картой.

По расчетному счету в дополнение к указанным выше сведениям необходимо запрашивать информацию о банковских картах, открытых по данному расчетному счету.

3. По электронным кошелькам (Qiwi, Яндекс.Деньги и др.):

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

4. По сайтам объявлений («Авито», «Авто» и др.).

Если мошенник выступает как продавец:

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

5. По социальным сетям:

- 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).

6. По доменному имени сайта:

- о паспортных данных регистратора доменного имени;
- использованных для регистрации абонентских номерах и электронных почтах;

- каким образом произведена регистрация пользователя;
- IP-адресах, использованных для регистрации доменного имени;
- IP-адресах, использованных для входа в личный кабинет или панель управления для администрирования доменного имени;

- оплате услуг регистрации и аренды доменного имени с указанием полных реквизитов плательщика.

7. По арендуемому хостингу:

- о паспортных данных арендатора хостинга;
- использованных для аренды абонентских номерах и электронных почтах;

- каким образом была произведена регистрация пользователя;
- IP-адресах, использованных для аренды хостинга;
- IP-адресах, использованных для входа в личный кабинет или панель управления для администрирования хостинга;

- оплате услуг аренды хостинга с указанием полных реквизитов плательщика.

8. У интернет-провайдера: о пользователе и адресе использованного им оборудования, которому был выдан интересующий нас IP-адрес в интересующий нас промежуток времени.

9. По электронной почте:

- о паспортных данных владельца электронной почты;
- абонентских номерах, использованных для регистрации;
- IP-адресах, использованных для доступа к электронной почте за максимально известный период.

10. У провайдера SIP-телефонии:

- о паспортных данных владельца абонентского номера;
- использованных для регистрации абонентских номерах, электронных почтах;

- каким образом была произведена регистрация пользователя;
- IP-адресах, использованных для регистрации абонентского номера;

- IP-адресах, использованных для входа в личный кабинет, панель управления по администрированию данным абонентским номером;
- IP-адресах, использованных для осуществления звонков;
- абонентских номерах, на которые осуществлялась переадресация звонков;
- статистику звонков за интересующий период;
- информацию об оплате услуг связи с указанием полных реквизитов плательщика.

2.4. Действия сотрудников экспертно-криминалистического подразделения в процессе производства необходимых экспертиз с целью установления подозреваемых лиц, причастных к подготавливаемым или уже совершенным преступлениям в современном информационном пространстве с использованием сети Интернет

Эксперт-криминалист при поступлении первичных материалов, характеризующих преступление, совершенное в современном информационном пространстве с использованием сети Интернет (в большинстве своем это дистанционные хищения) проводит следующие действия:

1. При осмотре осуществляет процессуальные полномочия специалиста по обнаружению, закреплению и изъятию предметов в порядке, установленном ст. 58 УПК РФ.
2. Оказывает содействие следователю (дознавателю) в обнаружении, фиксации, изъятии, упаковке, а также сохранении предметов и следов преступления.
3. Проводит исследования предметов и следов на месте происшествия для получения сведений об обстоятельствах преступления и о лицах, причастных к его совершению.
4. Обсуждает со следователем (дознавателем), исходя из особенностей места происшествия, необходимость, целесообразность и последовательность применения тех или иных технических средств.
5. Оказывает содействие в полном и точном отражении в протоколе осмотра сведений, полученных в результате применения технических средств.
6. Принимает участие в выдвижении версий относительно произошедшего события и лиц, их совершивших.

2.5. Алгоритм контроля за принятием процессуального решения по сообщениям о преступлениях (происшествиях), совершенных в современном информационном пространстве с использованием сети Интернет²⁷

2.5.1. Старший дежурной смены дежурной части территориального органа МВД России на районном уровне ежедневно в ходе приема-сдачи дежурства осуществляет доклад начальнику территориального органа на районном уровне о сообщениях о преступлениях (происшествиях), совершенных дистанционным способом, по которым уголовные дела не возбуждены в дежурные сутки.

2.5.2. Начальник дежурной части территориального органа МВД России на районном уровне ежедневно предоставляет начальнику территориального органа на районном уровне сведения о зарегистрированных на территории оперативного обслуживания сообщениях о преступлениях указанной категории, процессуальное решение по которым не принято по истечении 3 суток.

2.5.3. Начальник территориального органа МВД России на районном уровне по истечении 3 суток с момента регистрации сообщений организует совместное заслушивание (с участием руководителей подразделений отдела уголовного розыска и следствия), в ходе которого определяет мероприятия, реализация которых необходима для принятия решения о возбуждении уголовного дела, закрепляет ответственных исполнителей. По материалам, срок рассмотрения которых продлен, начальником территориального органа МВД России на районном уровне принимаются дополнительные меры управленческого характера, направленные на недопущение продления срока рассмотрения сообщения свыше 10 суток, принятие законного и обоснованного процессуального решения.

2.5.4. Начальник дежурной части УМВД по АО ГУ МВД России по г. Москве еженедельно анализирует состояние работы по рассмотрению сообщений о преступлениях (происшествиях), совершенных дистанционным способом, и докладывает начальнику УМВД по АО ГУ МВД России по г. Москве о ее результатах для принятия управленческих решений по обеспечению своевременного возбуждения уголовных дел по ним, недопущению продления срока их рассмотрения свыше 10 суток.

2.5.5. Начальник дежурной части ГУ МВД России по г. Москве ежедневно докладывает заместителю начальника полиции ГУ МВД России по г. Москве о количестве сообщений о преступлениях (происшествиях), совершенных дистанционным способом, по которым уголовные дела не возбуждены в дежурные сутки.

²⁷ Разработанный ОУ ГУ МВД России по г. Москве алгоритм контроля за принятием процессуального решения по сообщениям о преступлениях (происшествиях), совершенных дистанционным способом, по которым уголовные дела не возбуждены в дежурные сутки, январь 2020 г.

2.6. Взаимодействие оперативных сотрудников и следователей при раскрытии и расследовании преступлений, совершенных в современном информационном пространстве с использованием сети Интернет

При составлении процессуальных документов по уголовным делам, связанным с обращением криптовалюты или аналогичными активами (таких как Bitcoin, Ethereum, Tether и пр.), следует обратить внимание на следующие аспекты (рис. 18).

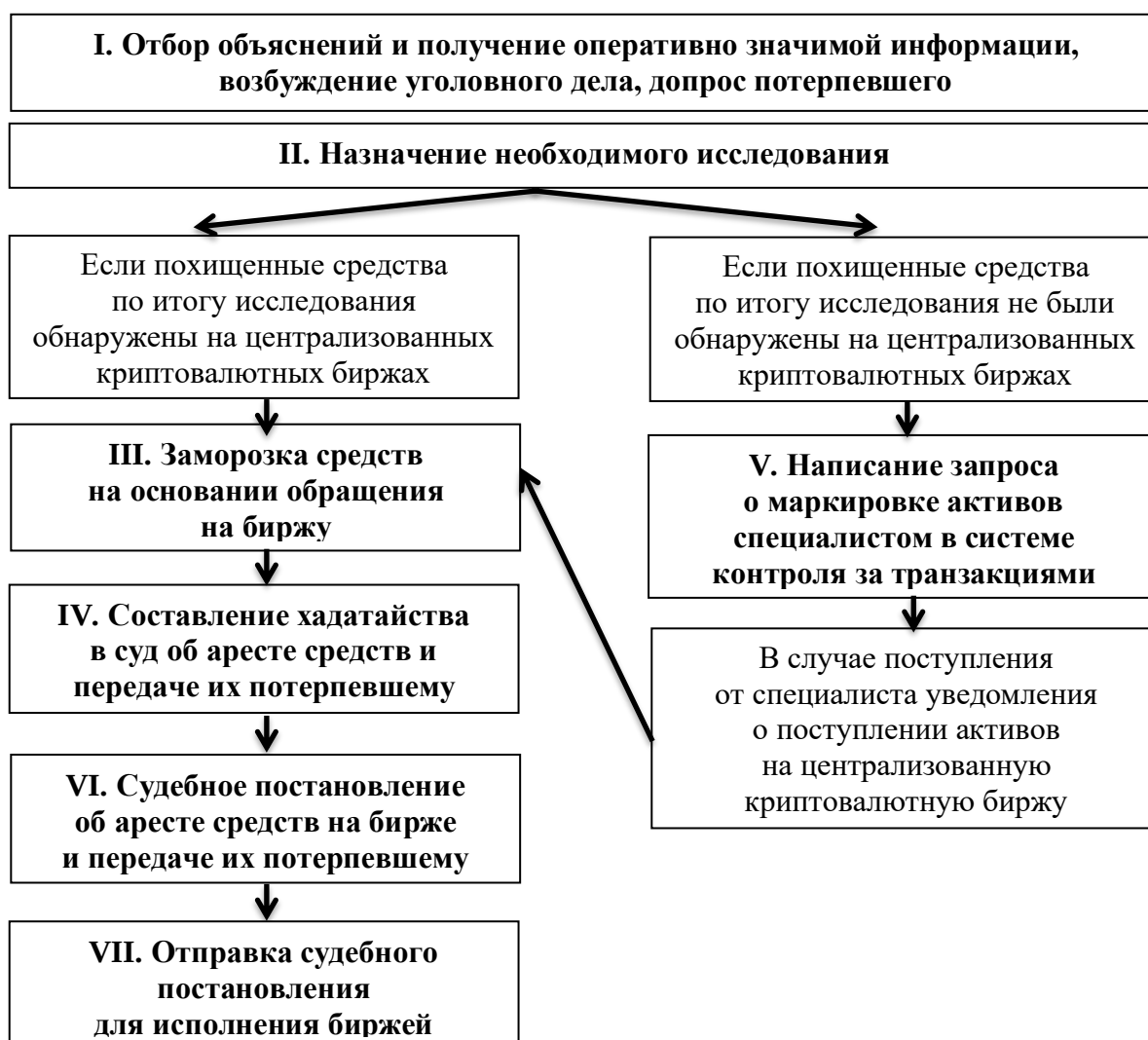


Рис. 18. Блок-схема работы по уголовным делам, связанным с обращением криптовалюты или аналогичными активами

1. При получении объяснений, возбуждении уголовного дела, допросе потерпевшего (см. рис. 19):

1. Установить, был ли осуществлен перевод средств злоумышленникам с криптовалютной биржи, если да – то какой и на какие данные (ФИО, телефон, электронная почта, идентификатор аккаунта) верифицирован аккаунт потерпевшего. В случае перевода с внебиржевых кошельков установить, каким программным обеспечением пользовался потерпевший и каким образом осуществлялась транзакция (сам потерпевший отправил активы злоумышленнику под воздействием злоупотребления доверием или злоумышленниками был получен доступ к управлению активами иным образом).

2. Зафиксировать в процессуальных документах суммы транзакций с указанием криптовалюты платежей, даты, времени, криптовалютного адреса получателя средств, а также по возможности получить хеш-идентификатор (он же Txid, id) и криптовалютный адрес отправителя средств.

3. В случае отправки средств, переводимых из национальной валюты любой формы, напрямую злоумышленникам по итогам обмена (когда потерпевший обменивает деньги с банковской карты на криптовалюту и напрямую указывает получателем криптовалютный адрес злоумышленника) – получить информацию о том, какой обменник совершил эту транзакцию, его максимально полные данные и контакты, а также сведения о том, почему потерпевший обратился именно в этот обменник (вероятно, его напрямую туда отправили злоумышленники).

4. К процессуальным документам по возможности приложить скриншоты совершения исходящих платежей с биржи (чаще всего находятся в истории выводов средств личного кабинета), историю пополнения средств на этой бирже (чаще всего находится в истории пополнений личного кабинета).

В настоящее время наиболее часто встречаются следующие криптоактивы:

– биткоин (Bitcoin, BTC), транзакции осуществляются в сети (блокчейне) Биткоин;

– эфириум (Эфир, Ethereum, Ether, ETH), транзакции осуществляются в сети (блокчейне) Эфириум;

– тезер (ЮСТД, Tether, USDT), транзакции чаще всего осуществляются в сети (блокчейне) Tron (TRC20, Tron Request for Comments 20, трон), но также может встречаться в сети (блокчейне) Эфириум (ERC20, Ethereum Request for Comments 20).

Важно верно указать сеть (блокчейн), где осуществляется транзакция, во всех процессуальных документах. Пример формулировки,

которая может быть использована в документах: криптовалютные активы в количестве 12.3456 Биткоина были похищены у ФИО с криптовалютной биржи Бинанс, где ранее находились у ФИО на аккаунте ID 123456, верифицированном на имя гражданина РФ ФИО с номером мобильного телефона 8 912 345-67-89 и адресом электронной почты 123456@yandex.ru.

Перевод средств ФИО совершил путем отправки неустановленному лицу средств из личного кабинета криптовалютной биржи Бинанс, осуществлялся тремя транзакциями в сети Биткоин:

– 986f5d8ac025bb542ec0604c46b632ab521269086e568518892b41cca98680b1 на адрес bc1qz0t7wy6rzt47vh8a4srcu6uupa6uh6h4l6cj6 06.02.2022 в 14:03 МСК в сумме 4.5 Биткоина;

– 1d70b34a9e3d98d3ebbe64d609ee68f2895b9665d6e6eec76817d40a47e52431 на адрес bc1qz0t7wy6rzt47vh8a4srcu6uupa6uh6h4l6cj6 06.02.2022 в 14:15 МСК в сумме 5.0 Биткоина;

– 26197a8c134cd858e5a5cc817dc827fefc1240c21018fda42763b7a481af614c на адрес bc1qz0t7wy6rzt47vh8a4srcu6uupa6uh6h4l6cj6 06.02.2022 в 14:20 МСК в сумме 2.8456 Биткоина.



Рис. 19. Допрос потерпевшего, свидетеля

II. При назначении специального исследования обращать внимание на верную описательную часть и постановку вопросов перед специалистом.

В описательной части запроса необходимо привести ранее полученную информацию о фактических обстоятельствах дела, имеющихся транзакциях и криптовалютных адресах. *Пример формулировки описательной части:*

Уголовное дело № 123456789 возбуждено _____ по признакам преступления, предусмотренного ч. 4 ст. 159 УК РФ в отношении неустановленных лиц.

Согласно материалам дела 06.02.2022 транзакциями с хеш-идентификаторами в сети Биткоин 986f5d8ac025bb542ec0604c46b632ab521269086e568518892b41cca98680b11d70b34a9e3d98d3ebbe64d609ee68f2895b9665d6e6eec76817d40a47e5243126197a8c134cd858e5a5cc817dc827fefc1240c21018fda42763b7a481af614c у ФИО похищена криптовалюта Биткоин в количестве 12.3456 Биткоинов с криптовалютной биржи Binance и переведена на адрес bc1qz0t7wy6rzt47vh8a4srcu6uурабуh6h4l6cj6.

В настоящий момент имеется необходимость получить дополнительные сведения о пути ее перемещения и адресах хранения указанных средств для целей полного и всестороннего исследования обстоятельств данного уголовного дела.

При постановке вопросов перед специалистом следует уделить внимание следующему:

1. Должны быть точно перечислены реквизиты транзакций (криптовалютные адреса получения, идентификаторы транзакций, по возможности – криптовалютный адрес отправки), желательно копировать данные сведения во избежание ошибок при перепечатывании.

2. Вопросы должны содержать интересующий период, за который нужно изучить блокчейн, чаще всего – с даты преступления до настоящего момента.

3. Необходимо ставить вопрос о поступлении полученных злоумышленниками средств на криптовалютные адреса, ассоциируемые с централизованными криптовалютными биржами.

4. Следует ставить вопрос о текущем порядке взаимодействия с централизованными криптовалютными биржами, которые будут установлены в ходе исследования.

5. Необходимо получить информацию о программном обеспечении, используемом при проведении специального исследования и номере его лицензии.

6. Дополнительно следует указывать на необходимость визуализации предоставленной информации при наличии к тому технической возможности.

Пример постановки вопросов перед специалистом:

Вопрос 1: возможно ли исследовать путь криптовалютных активов в сети Bitcoin, переданных транзакциями со следующими хеш-идентификаторами:

986f5d8ac025bb542ec0604c46b632ab521269086e568518892b41cca98680b11d70b34a9e3d98d3ebbe64d609ee68f2895b9665d6e6eec76817d40a47e5243126197a8c134cd858e5a5cc817dc827fefc1240c21018fda42763b7a481af614c на адрес bc1q0e6yltmh3n7a2ex57fu3a3jwx68l4rvzl6vjp? Если да, то какими техническими средствами и/или решениями это делается, какие номера лицензий специализированного программного обеспечения используются при проведении исследования?

Вопрос 2: имеется ли техническая возможность установить факт поступления криптовалютных активов, изначально переданных транзакциями, указанными в п. 1, на адреса централизованных криптовалютных бирж (или иных Virtual Asset Service Provider в значении, используемом межправительственной организацией с участием Российской Федерации «Группа разработки финансовых мер борьбы с отмыванием денег» (FATF)²⁸? Если да, то на каких криптовалютных биржах (или иных VASP) в настоящий момент находятся указанные криптовалютные активы, в каком количестве и какие они имеют реквизиты идентификации внутри криптовалютных бирж (или иных VASP)?

Вопрос 3: в случае невозможности установления факта поступления криптовалютных активов, изначально переданных транзакциями, указанными в п. 1, на адреса централизованных криптовалютных бирж (или иных VASP) полностью или в какой-то части, возможно ли установление каких-либо меток (маркировок) указанных криптовалютных активов с целью установления их последующих движений по биржам?

Вопрос 4: осуществляется ли в настоящий момент взаимодействие администрации централизованных криптовалютных бирж (или иных VASP) с российскими правоохранительными органами в части блокировки криптовалютных активов и их возврата потерпевшим по уголовным делам? Если да, то каким образом и в каких формах? Имеются ли рекомендации

о порядке взаимодействия с криптовалютными биржами (или иными VASP).

Дополнительно прошу предоставить визуализацию указанных сведений при наличии к тому технической возможности.

²⁸ Далее – VASP.

III. В случае наличия в исследовании информации о найденных активах на централизованных криптовалютных биржах следует обращаться с официальной почты МВД России к администрации соответствующей централизованной криптовалютной биржи тем способом, который будет указан в специальном исследовании, с требованием временной заморозки вывода криптовалютных активов с ассоциируемых с этой биржей криптовалютных адресов. В зависимости от конкретной криптовалютной биржи может потребоваться изменение формулировок или данных.

Этим же запросом следует запрашивать идентификационную и техническую информацию на лиц, связанных с использованием соответствующих аккаунтов криптовалютных бирж.

Пример подобного обращения следователя на централизованную криптовалютную биржу (может существенно отличаться в зависимости от конкретной криптовалютной биржи, необходимо уточнять детали у специалиста в каждом конкретном случае):

В производстве следственного отдела _____ находится уголовное дело № 123456789 по факту мошенничества в отношении ФИО.

Расследованием установлено, что последующие транзакции с похищенной криптовалютой взаимосвязаны со следующим адресом в сети Биткоин, принадлежащим бирже Binance inc.:bc1qz0t7wy6rztd47vh8a4srcuibuuh6h4l6cj6

На основании вышеизложенного и руководствуясь ч. 4 ст. 21 УПК РФ прошу Вас предоставить сведения об аккаунтах, которым выделялись указанные криптовалютные адреса, а именно: сведения о логине, телефоне, электронном почтовом ящике, указанные при регистрации; копии документов, представленных при верификации; информацию об IP-адресах, с которых осуществлялось обращение к указанным криптовалютным кошелькам; сведения о произведенных операциях по покупке и продаже криптовалюты с отражением объема и наименования криптовалюты, дат совершения операций, сведений об остатках криптовалюты.

На основании вышеизложенного прошу Вас приостановить операции с криптовалютой, находящейся на указанном выше адресе, а также иных адресах, принадлежащих этому лицу (или лицам) на срок до рассмотрения судом ходатайства о наложении ареста на имущество и вступления решения в силу, о чем будет сообщено дополнительно.

В настоящее время проводятся следственные действия и оперативно-розыскные мероприятия, направленные на проверку финансовых операций, проведенных с использованием криптовалютных кошельков, и установление похищенного имущества.

В связи с ограниченными сроками расследования указанные сведения прошу предоставить в кратчайшие сроки, направив на адрес служебной электронной почты: «_____@mvd.ru».

IV. В случае успешной заморозки криптовалютных активов на централизованной криптовалютной бирже необходимо получение в суде постановления об аресте указанных средств. При составлении подобного ходатайства необходимо указать, какие криптовалютные адреса на основании специального исследования были выявлены и к каким централизованным криптовалютным биржам они отнесены.

Примерный текст для включения в ходатайство.

Как следует из материалов дела, похищенные у ФИО криптовалютные активы были выведены транзакциями со следующими хеш-идентификаторами в сети Биткоин – 986f5d8ac025bb542ec0604c46b632ab521269086e568518892b41cca98680b11d70b34a9e3d98d3ebbe64d609ee68f2895b9665d6e6eec76817d40a47e5243126197a8c134cd858e5a5cc817dc827fefc1240c21018fda42763b7a481af614c – на криптовалютный адрес bc1q0e6yltmlh3n7a2ex57fu3a3jwx68l4rvzl6vjp. Специальным исследованием № 123 от 10 февраля 2022 г. было установлено, что указанные средства поступили на криптовалютный адрес bc1qz0t7wy6rztd47vh8a4srcu6uypa6uh6h4l6cjb, принадлежащий централизованной криптовалютной бирже Binance inc.

На основании вышеизложенного и руководствуясь п. «б» ч. 3.1 ст. 82, ст. 115 УПК РФ прошу наложить арест на криптовалютные средства, находящиеся на аккаунте централизованной криптовалютной биржи Binance inc. и ассоциированных с данным аккаунтом адресах иных криптовалютных активов указанной централизованной криптовалютной биржи, и передать их ФИО.

V. В случае отсутствия в исследовании информации о наличии похищенных активов на криптовалютных адресах, связанных с централизованными криптовалютными биржами или в случае частичного нахождения средств на таких адресах следует обратиться к специалисту с официальным запросом на маркировку указанных криптовалютных адресов с целью установления дальнейшего движения этих средств.

Примерный текст обращения.

В производстве следственного отдела _____ находится уголовное дело № 123456789 по факту мошенничества в отношении ФИО.

Специальным исследованием от 10 февраля 2022 г. № 123 было установлено, что похищенные транзакциями со следующими хеш-идентификаторами
986f5d8ac025bb542ec0604c46b632ab521269086e568518892b41cca98680b11d70b34a9e3d98d3ebbe64d609ee68f2895b9665d6e6eec76817d40a47e524

3126197a8c134cd858e5a5cc817dc827fefc1240c21018fda42763b7a481af614с средства после поступления на криптовалютный адрес злоумышленников bc1q0e6yltmlh3n7a2ex57fu3a3jwx68l4rvzl6vjp были в последующем распределены по криптовалютным адресам bc1q5gvpffrc3vachg60m8qfvv79g8u5a49de6g064 и 1NE5ZRtau574x6kA5m34v7WcCCQYmQpzPf, которые в настоящий момент не ассоциируются с какими-либо централизованными криптовалютными биржами.

На основании вышеизложенного прошу Вас надлежащим образом маркировать указанные криптовалютные адреса и незамедлительно сообщить о движении криптовалютных активов с указанных криптовалютных адресов по электронной почте «_____@mvd.ru» или телефону 8 923 232-32-32.

VI. Судебное постановление должно, среди прочего, содержать следующую информацию:

- 1) данные о проведенном исследовании и его выводах;
- 2) указание хеш-идентификаторов транзакций и криптовалютных адресов злоумышленников;
- 3) данные о конечных адресах поступления на централизованную криптовалютную биржу, где ранее были заморожены активы.

При наличии к тому необходимости полный текст описания движения криптоактивов содержится в описательной части специального исследования и может быть взят оттуда путем копирования текста во избежание опечаток при ручном переносе данных.

VII. После получения судебного постановления потерпевший должен самостоятельно открыть аккаунты на соответствующих централизованных криптовалютных биржах и пройти там полную верификацию. Данные такого аккаунта должны быть переданы бирже вместе с сопроводительным письмом к судебному постановлению через официальную электронную почту МВД. Текст сопроводительного письма может отличаться в зависимости от конкретной биржи. Перед отправкой желательно согласовывать содержание сопроводительного письма со специалистом.

Примерный текст сопроводительного письма.

Направляю Вам для исполнения постановление Басманного суда Москвы от 15 февраля 2022 г. по делу №111111/22 и реквизиты аккаунта потерпевшего ФИО для перевода ему криптовалютных активов в количестве 12.3456 Биткойна.

Глава 3.
Особенности получения
оперативно значимой информации
сотрудниками оперативных подразделений
и следственных органов в целях раскрытия преступлений,
совершаемых в современном информационном пространстве
с использованием сети Интернет

3.1. Алгоритм действий
оперативных сотрудников и следователей,
направленных на получение необходимой информации
у сторонних компаний, организаций и учреждений

Сведения, запрашиваемые у операторов сотовой связи:

- 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 сим-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;
- информация о входящих и исходящих платежах по лицевому счету абонентского номера;
- информация об IP-адресах, использованных для входа в личный кабинет сотового оператора по управлению данным номером, так как в большинстве случаев мошенник использует абонентские номера, зарегистрированные на подставных лиц, и все операции по управлению абонентским номером проводит через личный кабинет, тем самым оставляя «след» в виде своего IP-адреса;
- копия регистрационной формы – документ, который заполняет продавец сим-карты при ее регистрации. Помимо установочных данных мы узнаем данные об адресе торговой точки, где она была реализована, а также данные продавца. К этому лицу у следствия должны возникнуть обоснованные вопросы.

Сведения, запрашиваемые по банковским картам и расчетным счетам:

По банковской карте:

- паспортные данные владельца банковской карты;
- информация о движении денежных средств по банковской карте и местах их обналичивания за последние полгода с указанием точного времени проведения приходных и расходных операций, номеров и кодов 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, где совершались покупки. Каждый интернет-магазин предоставит информацию об адресе мошенника, на который почтовым переводом был отправлен приобретенный товар;
- абонентские номера, привязанные к данной банковской карте услугой «Мобильного банка», где и каким образом они были подключены;
- адрес офиса банка, в котором была открыта банковская карта;
- IP-адреса, использованные для входа в онлайн-сервис по управлению данной банковской картой.

По расчетному счету необходимо запрашивать аналогичную информацию о банковских картах, открытых по данному расчетному счету.

Сведения, запрашиваемые по электронным кошелькам (Qiwi, Яндекс.Деньги и др.):

- паспортные данные владельца электронного кошелька;
- способ и место идентификации электронного кошелька;
- абонентский номер, с использованием которого был создан электронный кошелек;
- абонентские номера, привязанные к электронному кошельку;
- виртуальные банковские карты, выпущенные по данному электронному кошельку;
- пластиковые карты, выпущенные по данному кошельку, способ их получения (адрес почтового отправления);

- входящие и исходящие платежи по электронному кошельку с момента его регистрации;
- IP-адреса, использованные для совершения денежных транзакций, а также администрирования электронного кошелька.

Сведения, запрашиваемые по сайтам объявлений («Авито», «Юла» и др.)

Если мошенник выступает как продавец:

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

Если мошенник выступает как покупатель:

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

Сведения, запрашиваемые по социальным сетям:

- информация о пользователе страницы социальной сети (ссылка на страницу, например <https://vk.com/id410077130>);
- установочные данные, использованные им для регистрации абонентского номера и электронной почты;
- IP-адреса, использованные для создания и доступа к странице за последние два месяца;
- аналогичная информация 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).

Сведения, запрашиваемые по доменному имени сайта:

- паспортные данные регистратора доменного имени;
- использованные для регистрации абонентские номера и электронные почты;
- каким образом произведена регистрация пользователя;
- IP-адреса, использованные для регистрации доменного имени;
- IP-адреса, использованные для входа в личный кабинет или панель управления для администрирования доменного имени;
- информация об оплате услуг регистрации и аренды доменного имени с указанием полных реквизитов плательщика;
- аналогичная информация по иным доменным именам, зарегистрированным данным пользователем, установленным при анализе Cookie-файлов.

Сведения, запрашиваемые по арендуемому хостингу:

- паспортные данные арендатора хостинга;
- использованные для аренды абонентские номера и электронные почты;
- каким образом произведена регистрация пользователя;
- IP-адреса, использованные для аренды хостинга;
- IP-адреса, использованные для входа в личный кабинет или панель управления для администрирования хостинга;
- информация об оплате услуг аренды хостинга с указанием полных реквизитов плательщика;
- аналогичная информация по иным хостингам, арендуемым данным пользователем, установленным при анализе Cookie-файлов.

Сведения, запрашиваемые у интернет-провайдера:

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

Сведения, запрашиваемые по электронной почте:

- паспортные данные владельца электронной почты;
- абонентские номера, использованные для регистрации;

- IP-адреса, использованные для доступа к электронной почте за максимально известный период;
- аналогичная информация по иным электронным почтам, зарегистрированным данным пользователем, установленным при анализе Cookie-файлов.

Сведения, запрашиваемые у провайдера SIP-телефонии:

- паспортные данные владельца абонентского номера;
- использованные для регистрации абонентские номера, электронные почты;
- каким образом была произведена регистрация пользователя;
- IP-адреса, использованные для регистрации абонентского номера;
- IP-адреса, использованные для входа в личный кабинет, панель управления по администрированию данным абонентским номером;
- IP-адреса, использованные для осуществления звонков;
- абонентские номера, использующие переадресацию входящих вызовов;
- статистика звонков за интересующий период;
- информация об оплате услуг связи с указанием полных реквизитов плательщика.

3.2. Схемы расследования наиболее распространённых преступлений, совершаемых в современном информационном пространстве с использованием сети Интернет

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 (см. рис. 20, 21).

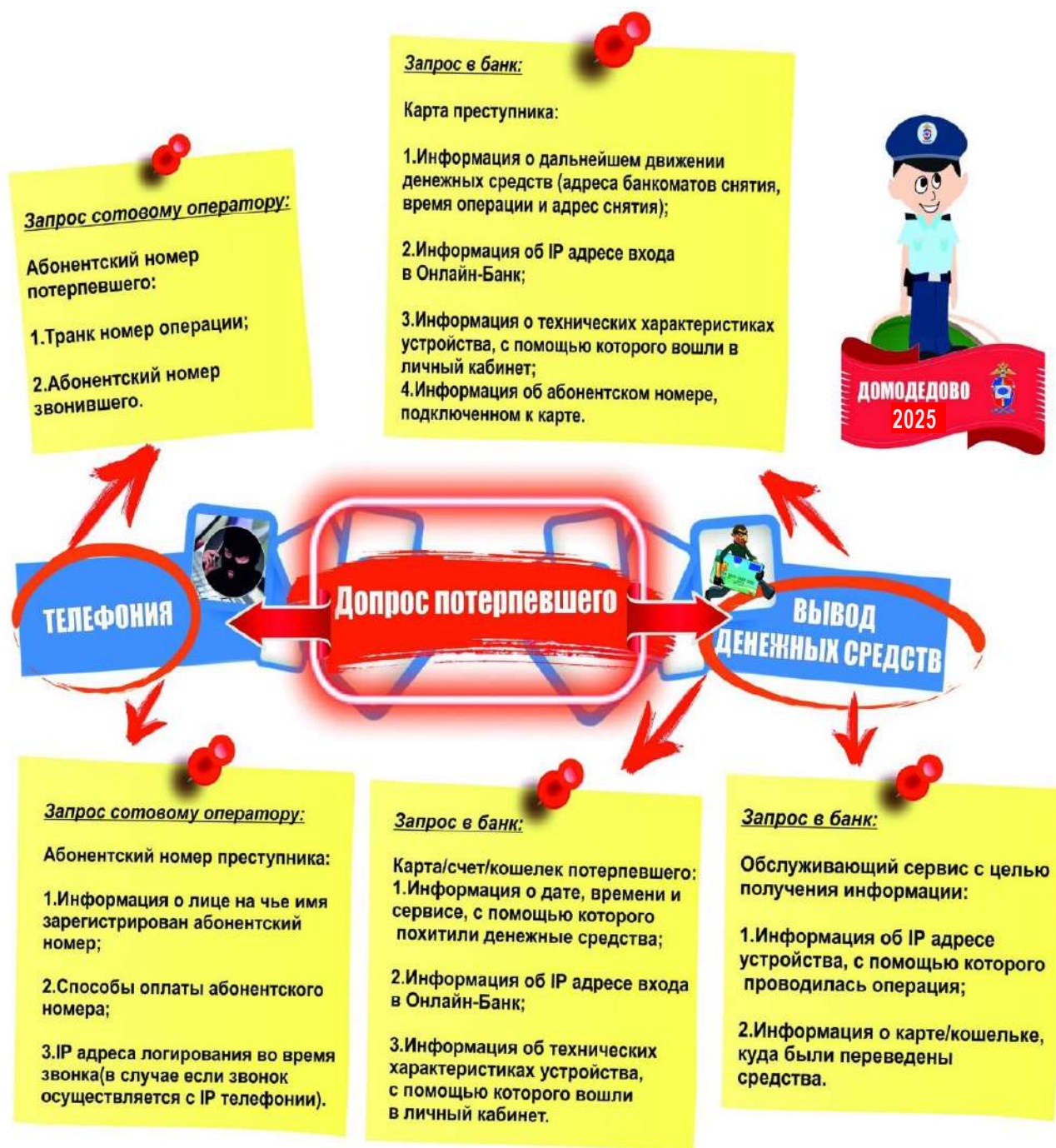


Рис. 20. Схема запросов сотовому оператору и в банк

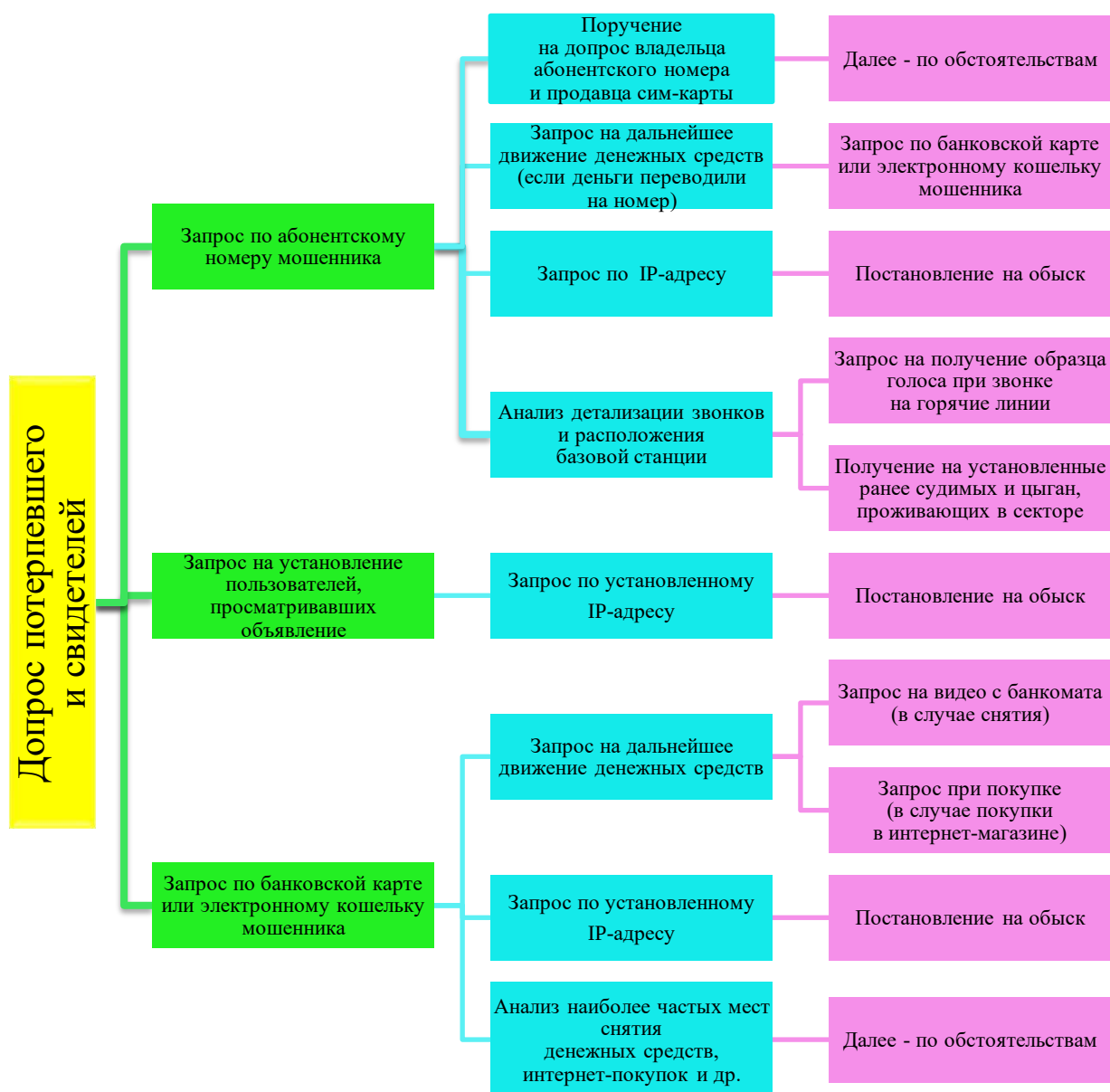


Рис. 21. Порядок действий сотрудника органов внутренних дел при раскрытии мошенничества через сайты объявлений (мошенник – продавец)

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, осуществляет перевод через онлайн-сервисы и совершает покупку, или же мошенник просит подойти к банкомату и выполнить ряд комбинаций, подключая «Мобильный банк» и в последующем похищая денежные средства (см. рис. 22).

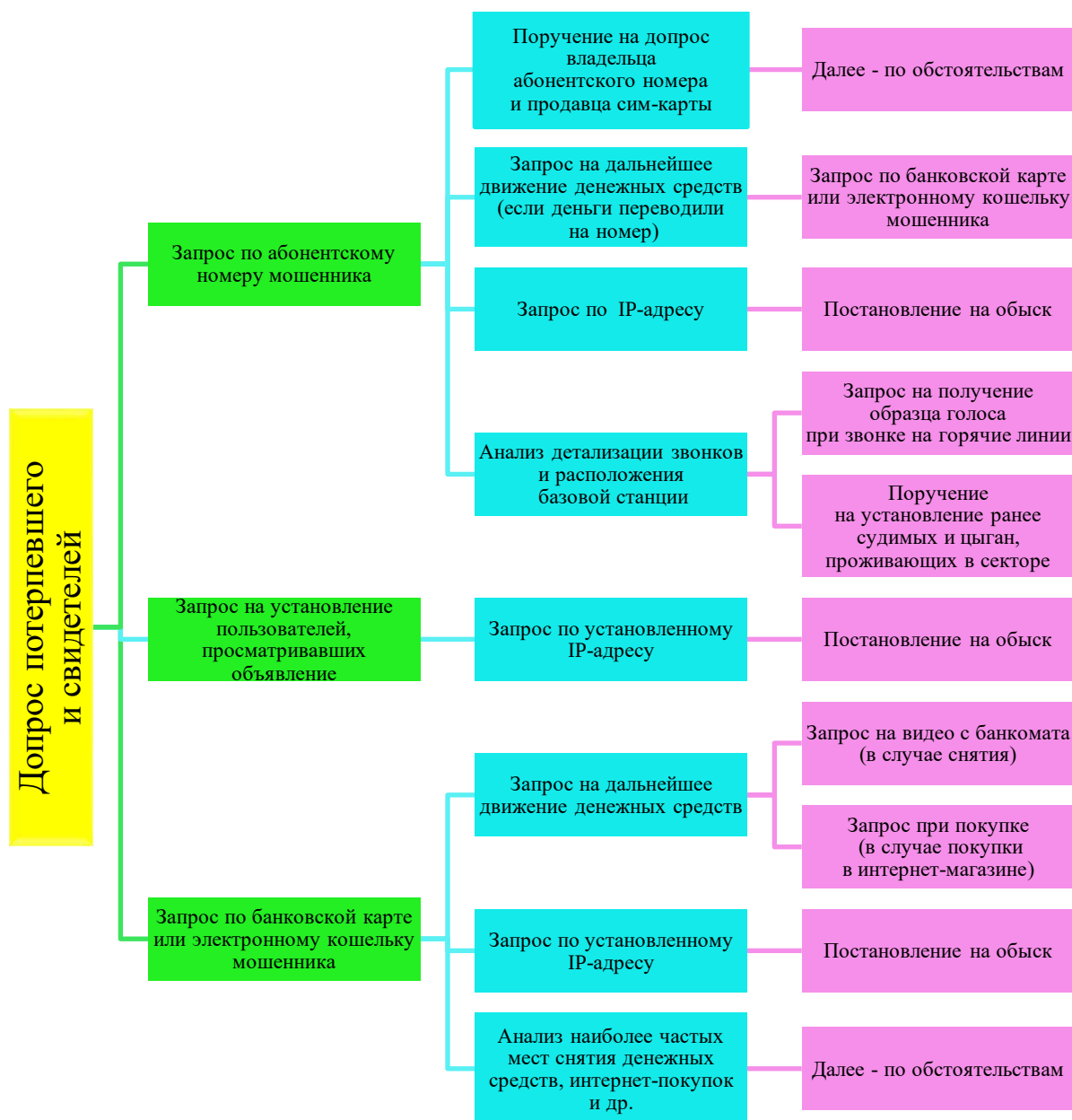


Рис. 22. Порядок действий сотрудника органов внутренних дел при раскрытии мошенничества через сайты объявлений (мошенник – покупатель)

Мошенничества через сайты объявлений.

Мошенник-покупатель использует для введения в заблуждение ссылку, присланную потерпевшему

Преступник, непосредственно осуществляющий общение с потерпевшим, ищет объявление о продаже товара, создает ссылку путем движения по меню бота с возможностью создания простейшей страницы в сети с указанием номера объявления и данных о стоимости товара, а также

адресе доставки, после чего в ходе переписки либо телефонного общения вводит в заблуждение потерпевшего и сообщает о том, что хочет приобрести товар. Далее направляет заранее подготовленную ссылку потерпевшему, который переходит по ней и видит данные своего товара и лейбл Авито, Юла, скопированный с официального сайта, далее нажимает на кнопку «оплатить» и переходит на сервис *Card2Card* какого-либо банка.

В некоторых случаях ссылка потерпевшему перенаправляется путем направления электронного письма на почтовый ящик, имитирующий название торговой площадки либо службы доставки. В данном случае необходимо направить запрос в службу, зарегистрировавшую электронный ящик, с целью получения анкетных данных клиента, способов оплаты услуги, информации об иных ящиках, зарегистрированных на данного клиента, IP-адресах администрирования в личном кабинете.

Не менее важная информация заключена в самой ссылке, состоящей из доменного имени и набора цифр и букв, ведущих к адресу URL, то есть к IP-адресу хостинга, на котором находится информация. В случае, если доменное имя принадлежит российскому регистратору, необходимо направить запрос в данную организацию с целью получения анкетных данных, способов оплаты, IP-адресов администрирования в личном кабинете. Полученная информация может способствовать установлению лица, создавшего бот, используемый для совершения преступления (см. рис. 23).

Допрос потерпевшего, свидетеля

Телефония: запрос оператору: 1) данные клиента, с которым заключен договор о предоставлении услуг связи. 2) детализация соединений абонентского номера на предмет установления IMEI-номера активации услуг мессенджера (в случае, если переписка велась в нем); 3) способы оплаты абонентского номера за период активации мессенджера	Запрос в банк с целью получения информации о выводе денежных средств: 1) информация о движении денежных средств потерпевшего; 2) информация об IP-адресе администрирования счета/карты/кошелька на который переводились денежные средства; 3) информация о движении денежных средств по карте/кошельку/счету	Запрос в компанию интернет-провайдера по ссылке: 1) предварительно на сервисе Whois информация об организации регистратора доменного имени и IP-адресе хостинга сервера, на котором расположена страница; 2) информация об анкетных данных клиента, IP-адресах логирования и входа в личный кабинет, способах оплаты услуги, иных предоставляемых услугах клиенту
--	---	--

Рис. 23. Порядок действий сотрудника органов внутренних дел при раскрытии мошенничества через сайты объявлений (с подменой сайта объявлений)

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 предлогами (заболел родственник, не хватает на срочную покупку и т. д.) (см. рис. 24).

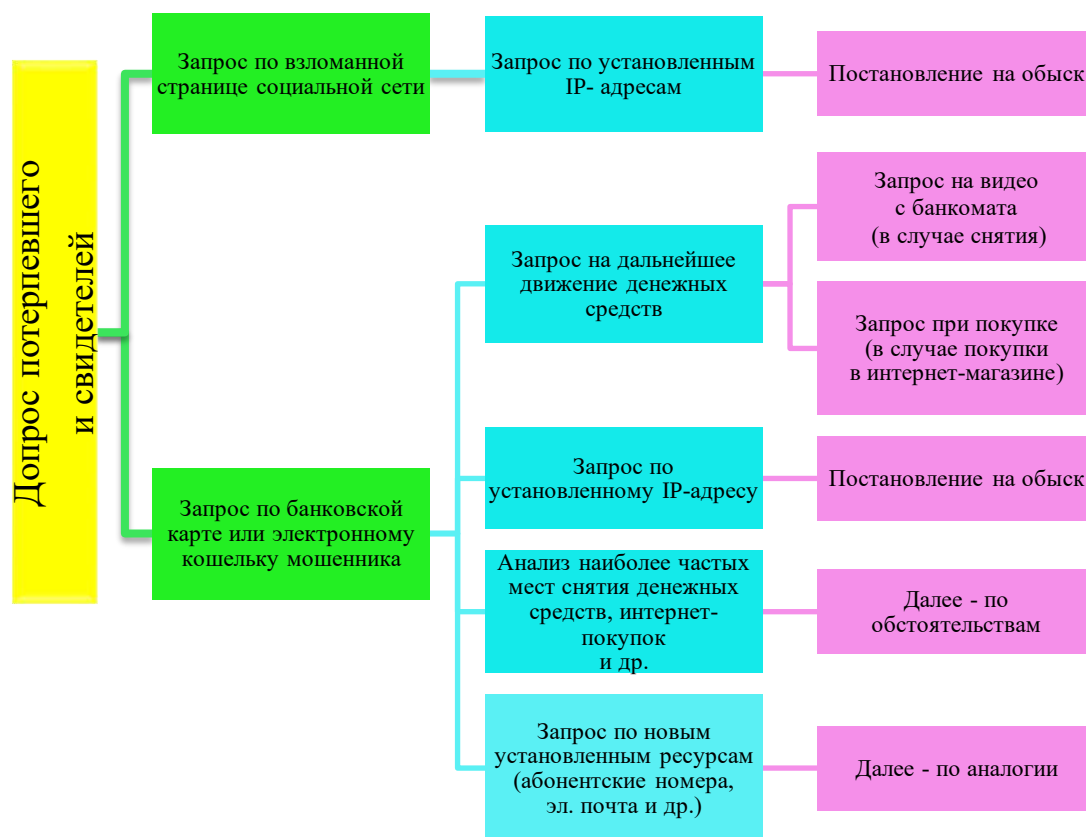


Рис. 24. Порядок действий сотрудника органов внутренних дел при раскрытии мошенничества путем взлома страниц социальных сетей

Мошенничества, совершенные 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 (см. рис. 25).

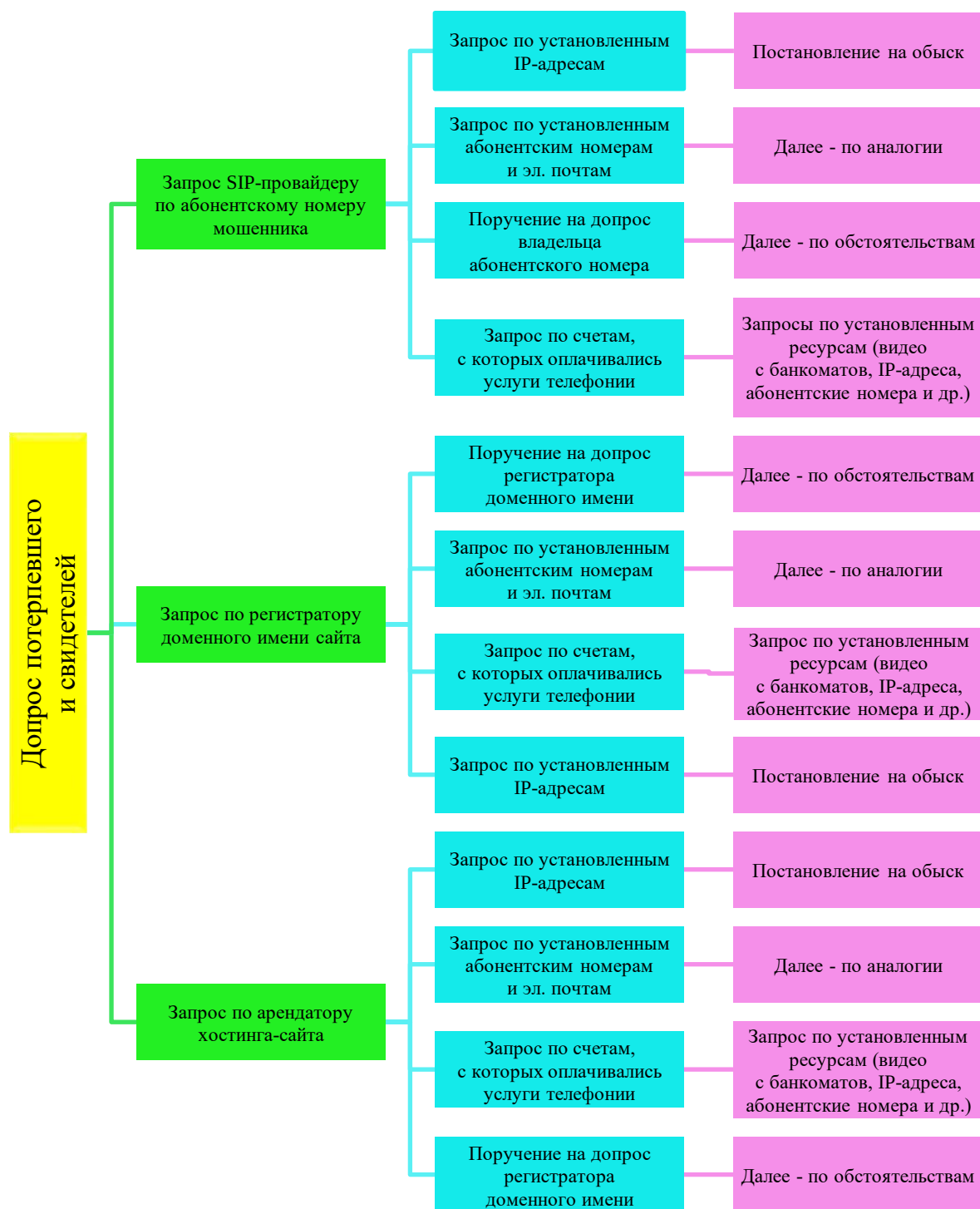


Рис. 25. Порядок действий сотрудника органов внутренних дел при раскрытии мошенничества с использованием интернет-сайтов

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 с представителем компании, и спрашивает его телефон. В последующем связывается с представителем и просит последнего по пути пополнить счет абонентского номера (или банковской карты) на некоторую сумму (рис. 26).

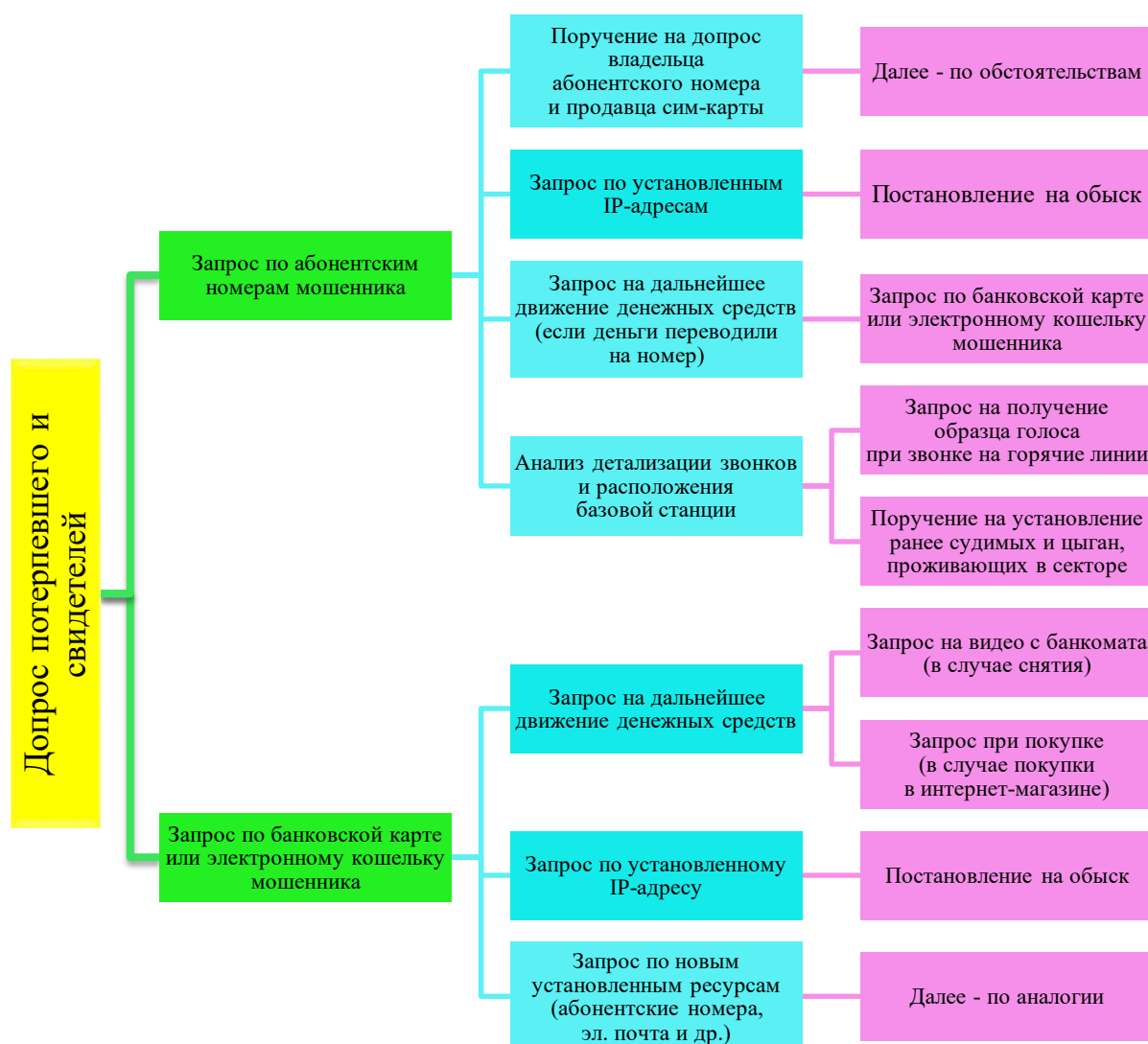


Рис. 26. Порядок действий сотрудника органов внутренних дел при раскрытии мошенничества, совершенного под предлогом заказа банкета

Мошенничество, совершенное под предлогом разблокировки банковской карты или предотвращения списания денежных средств

Мошенник осуществляет рассылку СМС-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 (рис. 27).

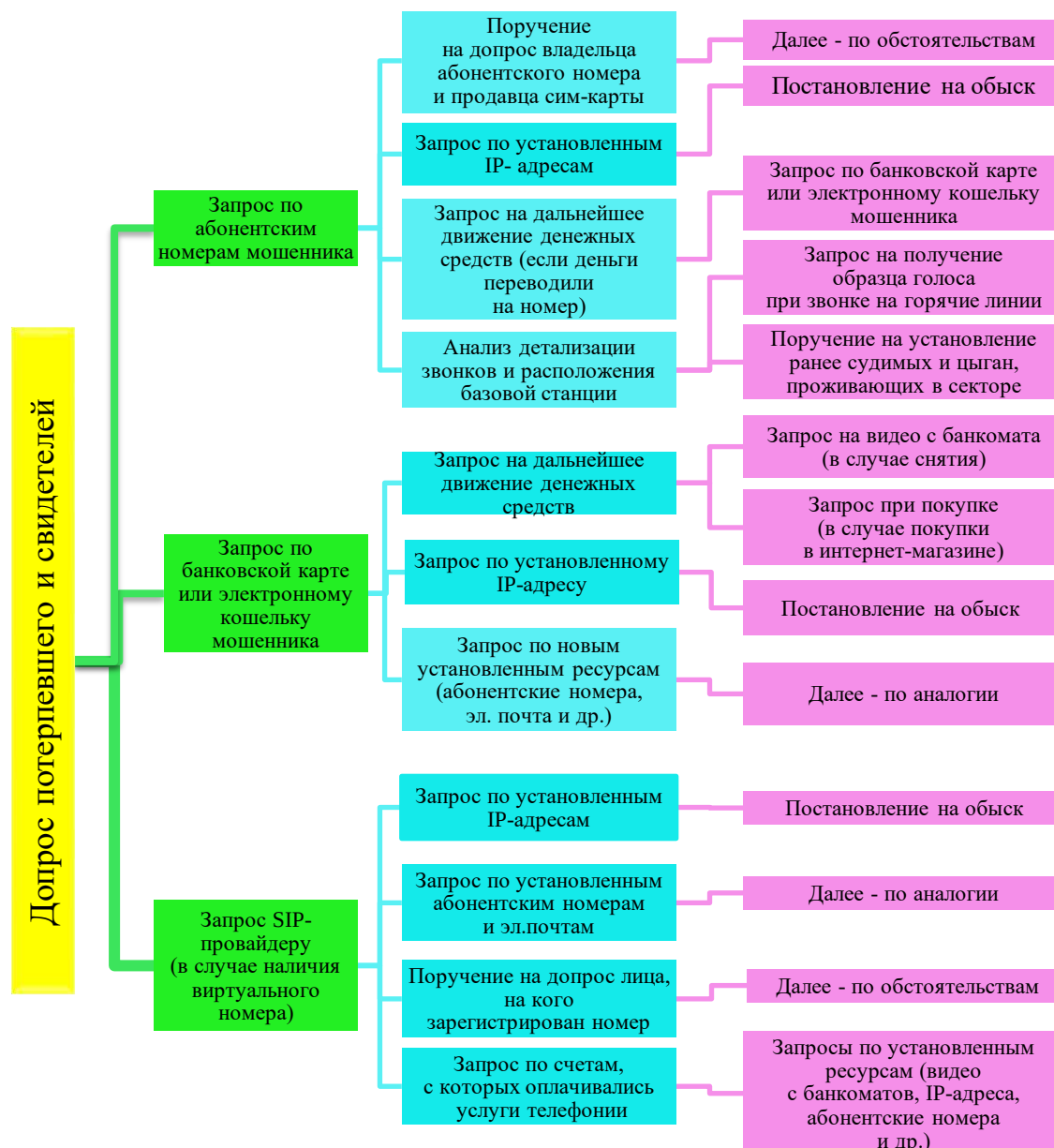


Рис. 27. Порядок действий сотрудника органов внутренних дел при раскрытии мошенничества под предлогом разблокировки банковской карты

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 (рис. 28).

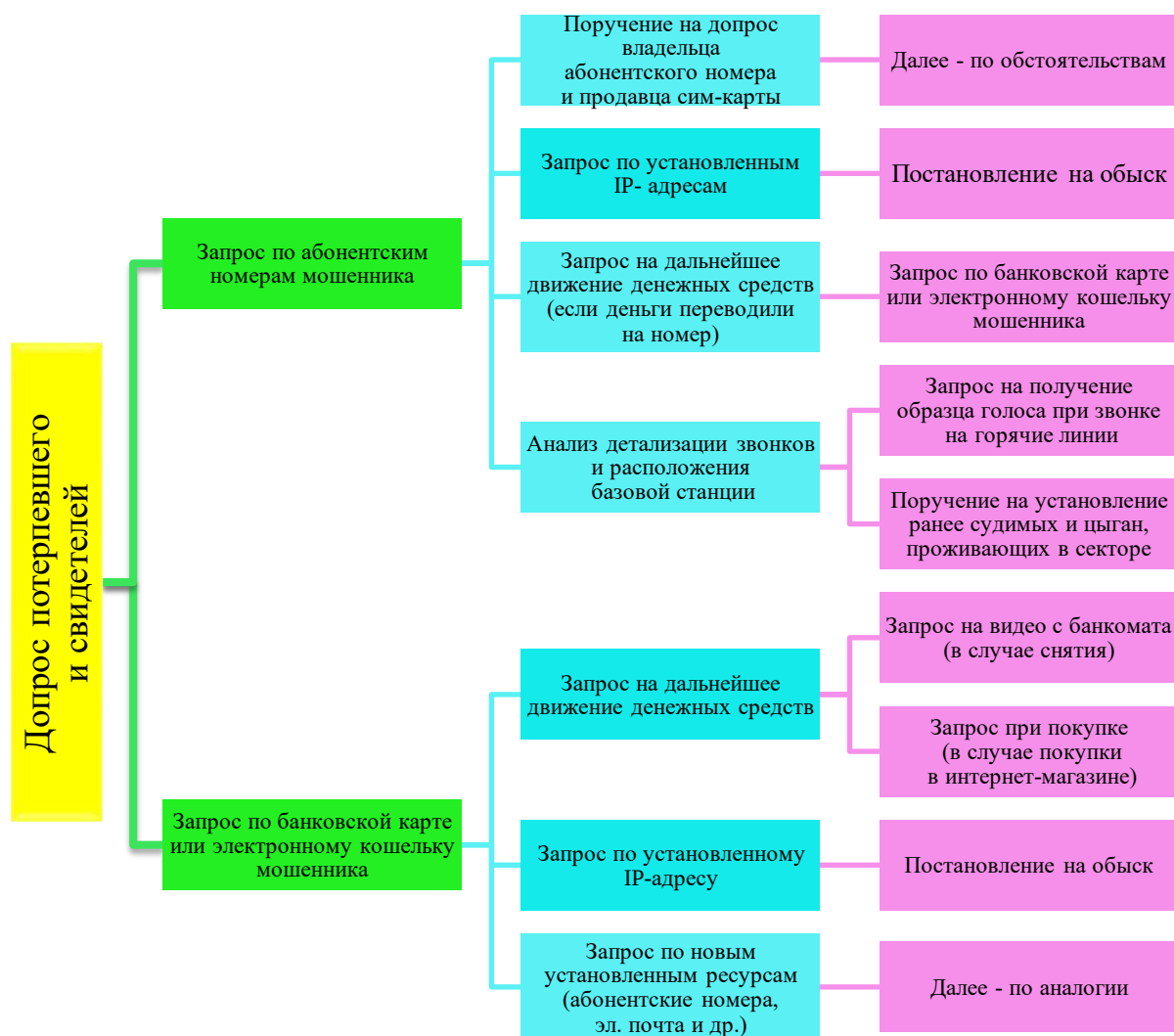


Рис. 28. Порядок действий сотрудника органов внутренних дел при раскрытии мошенничества, совершенного под предлогом помощи родственнику, попавшему в беду

Мошенничество, совершенное под предлогом компенсации за ранее приобретенные БАДы

На стационарный или абонентский номер потерпевшего звонит мошенник, представляется сотрудником прокуратуры или правоохранительных органов и сообщает, что в настоящий момент задержана группа мошенников, продававших некачественные БАДы²⁹, и потерпевшему положена компенсация. Однако для ее получения необходимо оплатить государственную пошлину или налоговый сбор (рис. 29).

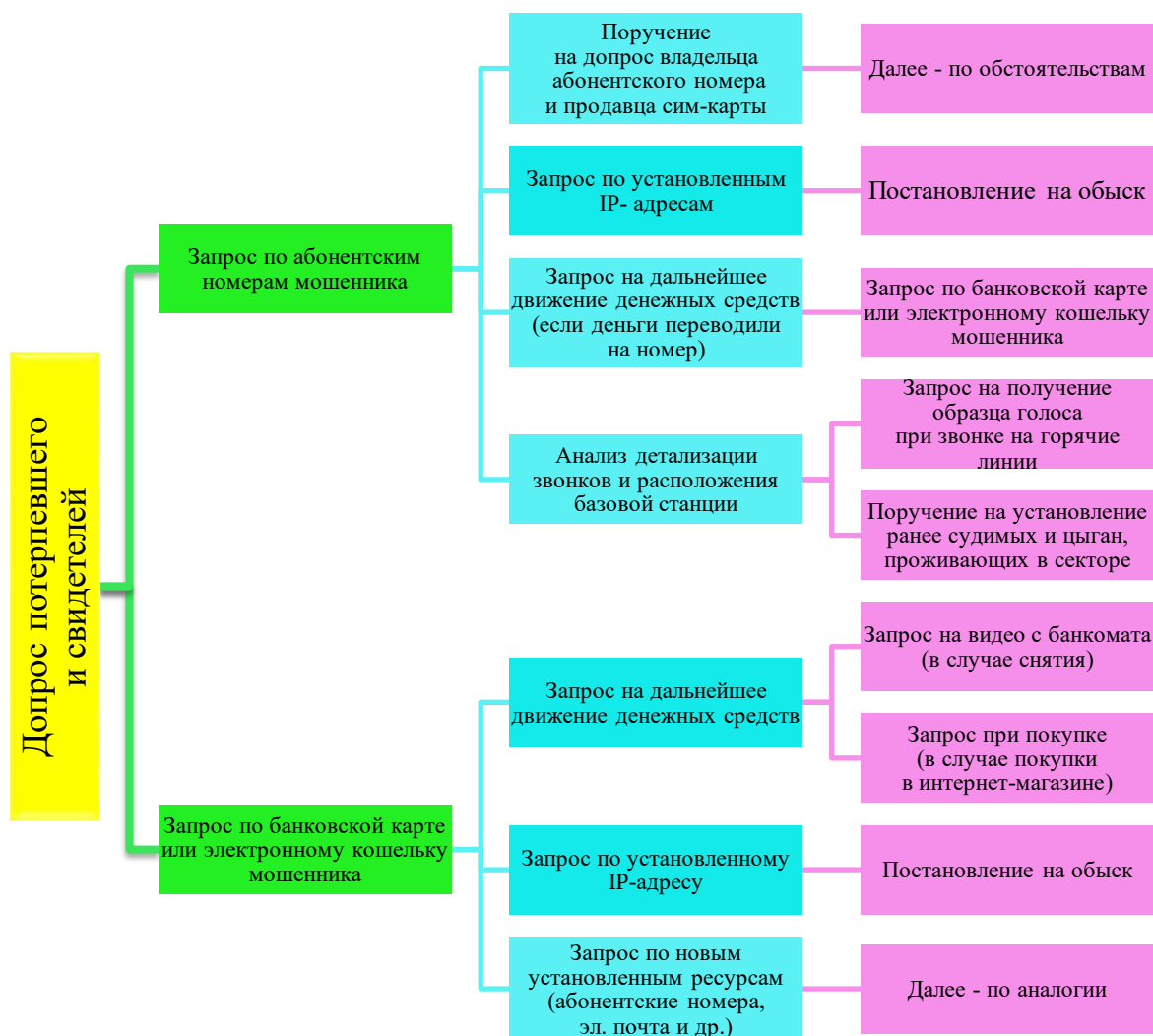


Рис. 29. Порядок действий сотрудника органов внутренних дел при раскрытии мошенничества, совершенного под предлогом компенсации за ранее приобретенные БАДы

²⁹ Биологические активные добавки и их композиции предназначены для непосредственного приема с пищей или введения в состав пищевых продуктов. БАД используется как дополнительный источник биологически активных веществ (пищевых волокон, витаминов, минеральных веществ, аминокислот) для ликвидации их дефицита в организме человека и оптимизации рационов питания. Стандартов по производству БАДов не существует, контроль их качества заключается лишь в оценке безопасности как пищевых продуктов.

Мошенничество, совершенное в современном информационном пространстве в сети Интернет 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/FriZksk)» или SMS-сообщение с текстом: «Смотри, как мы здорово получились на этой фотографии. Ссылка 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» (рис. 30).

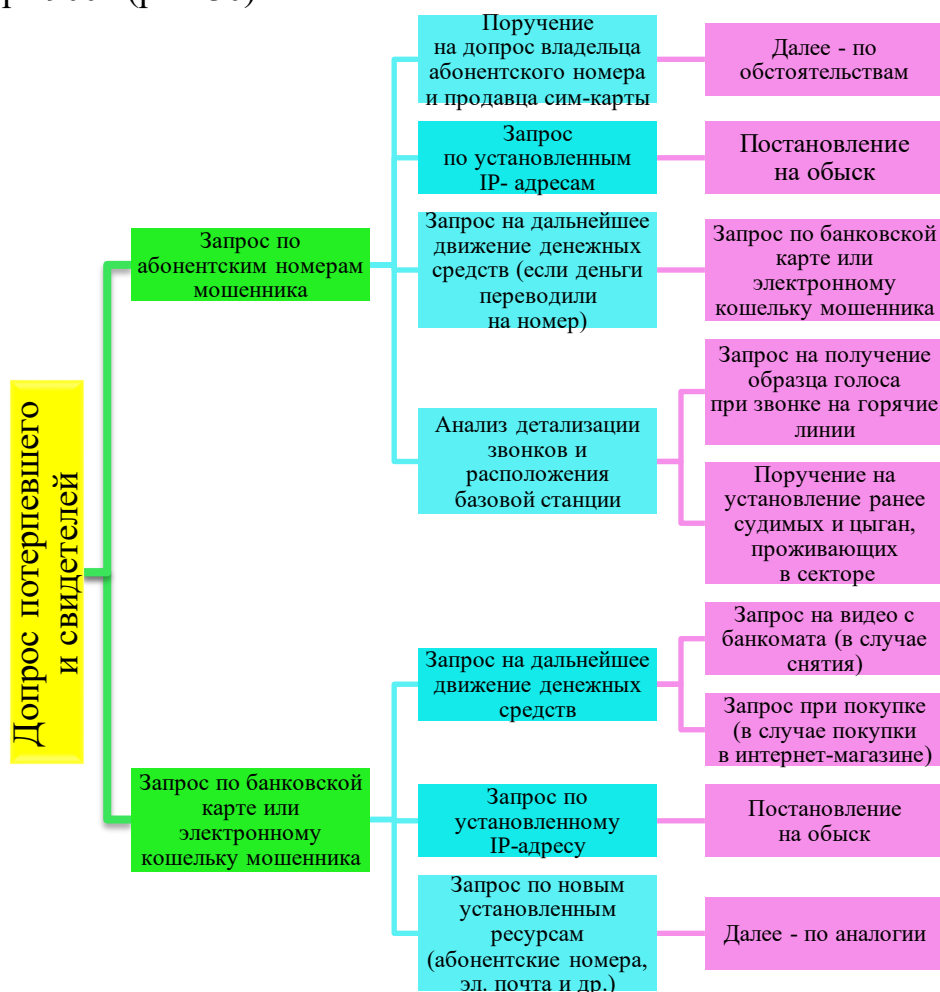


Рис. 30. Порядок действий сотрудника органов внутренних дел
при раскрытии мошенничества, совершенного с использованием вредоносных программ на ОС «Android»

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 (рис. 31).

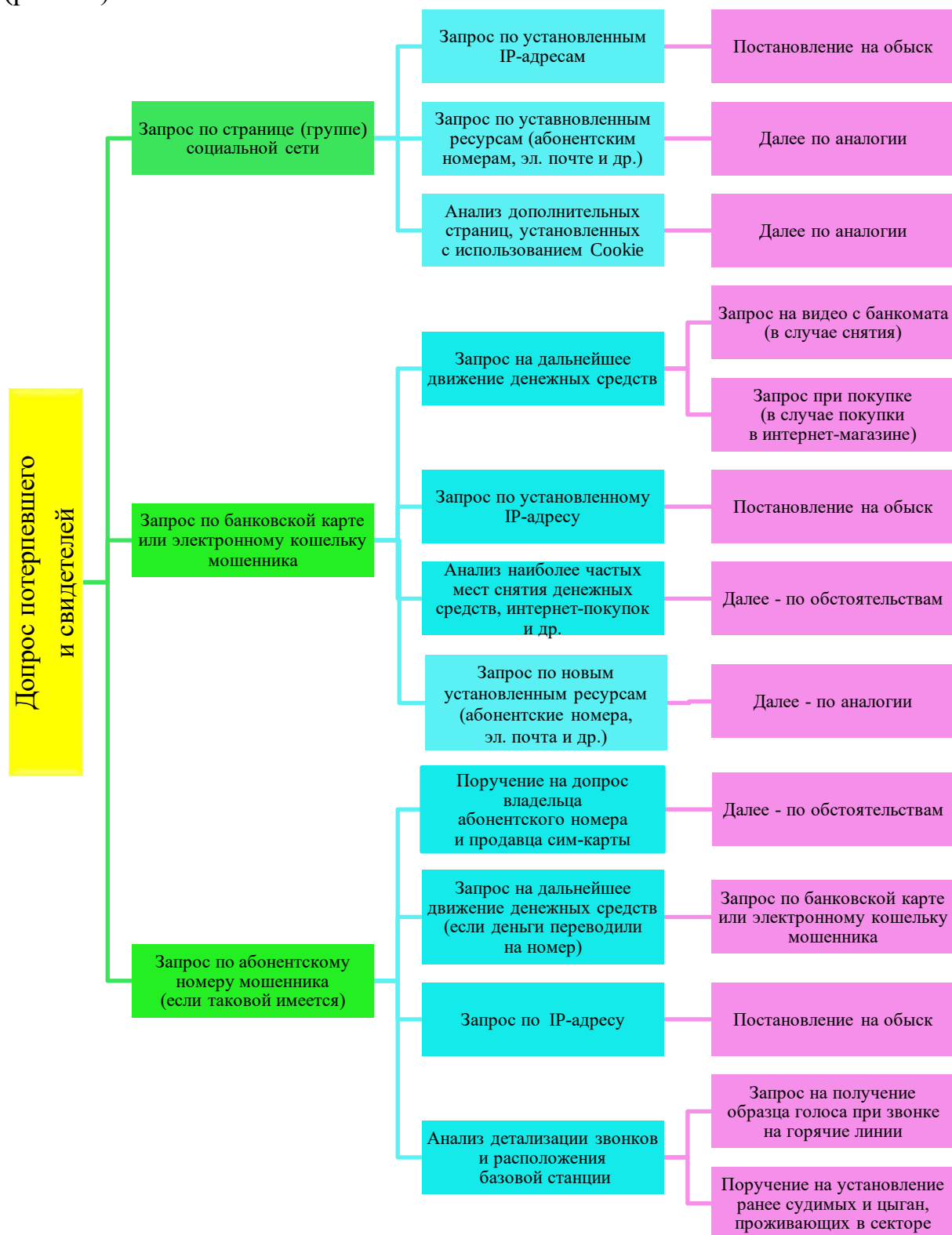


Рис. 31. Порядок действий сотрудника органов внутренних дел при раскрытии мошенничества, совершенного с использованием социальных сетей

**Раскрытие преступления, совершенного
от лица сотрудников банка,
сообщающих о проведении сомнительных операций**

Исходя из имеющегося опыта, очевидно, что звонки мошенников осуществляются из колл-центров, находящихся в большинстве случаев на территории стран ближнего зарубежья и других прилегающих к ним территориях. Это не значит, что установить преступников и задержать соучастников мы не можем.

Кроме информации о передвижении денежных средств со счетов потерпевших, имея знания об абонентских номерах, которые могут подменить преступники, становится возможным заранее иметь понимание о номере, с которого они звонят. Это, скорее всего, подмененный номер либо IP-телефония, либо абонентский номер оператора сотовой связи. Кроме того, большое значение имеет способ оплаты абонентского номера преступниками. Данная информация отсутствует в соответствующих отделах подразделений специальных технических мероприятий органов внутренних дел и ее надо запрашивать либо от следственных органов в рамках уголовного дела, либо путем получения разрешения на проведение ОРМ «Наведение справок».

В настоящее время большое значение имеет информация об устройстве и IP-адресе входа в банк-онлайн потерпевшего, если такой факт имел место. Данная информация непосредственно ведет нас к лицам, осуществляющим звонки потерпевшим, то есть к «звонарям».

Таким образом, работа должна проводиться по трем направлениям: телефония, движение похищенных денежных средств, устройства (IP, абонентские номера, IMEI мобильных устройств), с помощью которых переводили денежные средства со счета на счет (см. рис. 32).

Допрос потерпевшего				
Телефония		Вывод денежных средств		
Запрос сотовому оператору:	Запрос сотовому оператору:	Запрос в банк:	Запрос в банк:	Запрос в банк:
абонентский номер потерпевшего: транк-номер операции; абонентский номер звонившего	абонентский номер преступника: информация о лице, на чье имя зарегистрирован абонентский номер; способы оплаты абонентского номера; IP-адреса логирования во время звонка (в случае, если звонок осуществляется с IP- телефонии)	карта/счет/ кошелек потерпевшего: информация о дате, времени и сервисе, с помощью которого похитили денежные средства; информация об IP-адресе входа в онлайн-банк; информация о технических характеристиках устройства, с помощью которого вошли в личный кабинет	обслуживающий сервис с целью получения информации: информация об IP-адресе устройства, с помощью которого проводилась операция; информация о карте /кошельке, куда были переведены средства	карта преступника: информация о дальнейшем движении денежных средств (адреса банкоматов снятия, время операции и адрес снятия); информация об IP-адресе входа в онлайн- банк; информация о технических характеристи- ках устройства, с помощью которого вошли в личный кабинет; информация об абонентском номере, подключен- ном к карте

Рис. 32. Порядок действий сотрудника органов внутренних дел при раскрытии мошенничества, совершенного от лица сотрудников банка, сообщающих о проведении сомнительных операций

Мошенничество, совершенное с использованием разветвленной сети нелегальных узлов связи

В ходе проведения оперативно-розыскных мероприятий, направленных на раскрытие преступлений, совершаемых в современном информационном пространстве с использованием сети Интернет, в тесном взаимодействии с сотрудниками ФСБ России была разоблачена разветвленная сеть нелегальных узлов связи, действовавшая в 13 регионах России. Тысячи иностранных номеров телефонные мошенники маскировали под российские, обзванивали пострадавших, главным образом пенсионеров, убеждая их отдавать свои сбережения.

Телефонные мошенники отправляли сообщения на различные номера и предлагали будущим потенциальным жертвам заработать деньги. Так, сообщения направлялись от имени арбитражных специалистов, деятельность которых заключалась в обороте криптовалюты. Несостоявшийся криптовалютный трейдер³⁰ был взят с поличным. В г. Казани в результате проведения специальной операции столичной полицией, отследившей онлайн-переводы телефонных мошенников, была изъята банковская карта, на которой находилась часть похищенных денег в размере 1 млн руб. Деньги похитили у одной жительницы столичного района Марфино по классической схеме: 1) звонок якобы из поликлиники, в процессе которого были получены все необходимые данные потерпевшей; 2) звонок якобы от сотрудника полиции; 3) получение доступа к мобильному банку потерпевшей женщины; 4) перевод с ее счета 2 млн руб. Сообщника из г. Казани, который должен был покупать криптовалюту, использовали в темную через систему нелегальных автоматических «колл-центров».

В ходе проведения оперативно-розыскных мероприятий и следственных действий в съемных квартирах было обнаружено и изъято оборудование, называемое «SIM-бокс», – мобильные АТС, в реальном времени подменяющие телефонные номера. С таких устройств мошенники из Украины звонили на российские номера телефонов. В функции жителя из Казани входила своевременная замена сим-карт в соответствии с поступлением сведений на их замену. Задержано 26 операторов нелегальных АТС,

³⁰ *Трейдер* – торговец, человек, который занимается покупкой и продажей финансовых активов (акций, валют, облигаций, криптовалют, деривативов и т. д.) с целью получения прибыли. Основная деятельность трейдера заключается в спекуляции на финансовых рынках, т. е. в покупке активов по низкой цене и их последующей продаже по более высокой или наоборот – продажа по высокой цене с последующей покупкой по более низкой цене. Трейдеры могут работать сами на себя или обслуживать клиентов, например в банках. Профессиональные трейдеры обязательно имеют лицензию, которая позволяет заключать им сделки напрямую через биржу.

изъято 8 000 сим-карт, номера которых проходят по сотням нераскрытых преступлений, по которым возбуждены уголовные дела.

Одним из потерпевших был профессор МГУ Александр Демидов, пояснивший, что ему звонили от имени сотрудников ФСБ и сообщили о перечислении с его счетов террористам денежных сумм в размере 300 тыс. руб. Мошенники предложили профессору снять все имеющиеся на его счетах денежные средства и передать на проверку. Мужчина передал водителю такси 460 тыс. руб. При реализации плана спецоперации по задержанию мошенников все члены, входившие в организованную преступную группу, были задержаны (см. рис. 33).

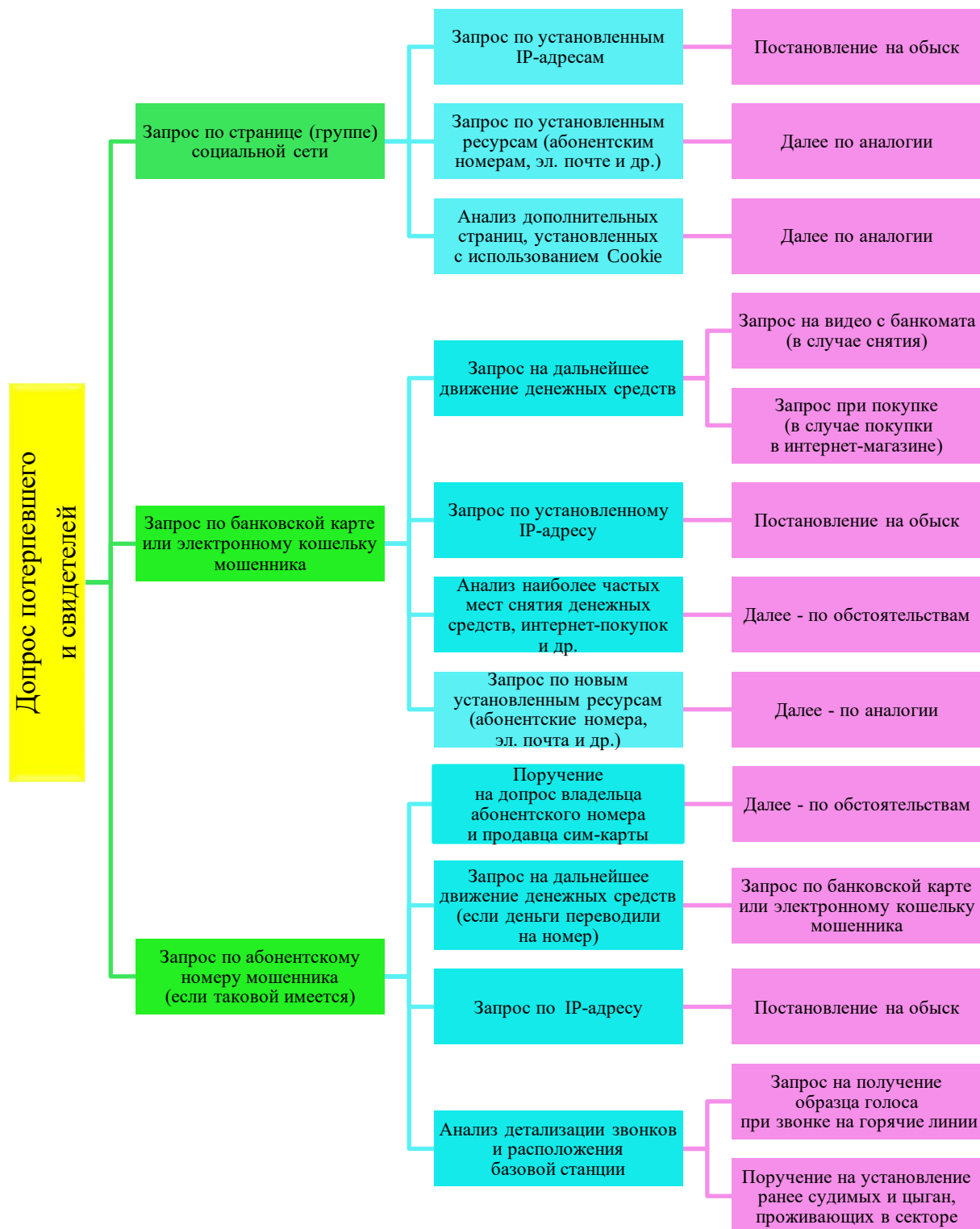


Рис. 33. Порядок действий сотрудника органов внутренних дел при раскрытии мошенничества, совершенного в современном информационном пространстве с использованием разветвленной сети нелегальных узлов связи

Мошенничество, совершенное в современном информационном пространстве с использованием различных мессенджеров

Предлагаем рассмотреть пример, именуемый «Поздравление с открыткой». Эксперты по кибербезопасности предупреждают о новом виде мошенничества. Изображения, например в виде милого котика и других различных видов животных, автомашин и т. п., на деле могут оказаться «троянским конем», куда вшиты так называемые фишинговые ссылки. Одно нажатие – и все данные банковской карты, госуслуг могут оказаться в руках мошенников. При этом они могут действовать от лица родственников, близких людей, друзей, знакомых. Не стоит также открывать архивы, под их видом злоумышленники рассылают вредоносное программное обеспечение. Необходимо быть осторожным и предупредить близких! (см. рис. 34).

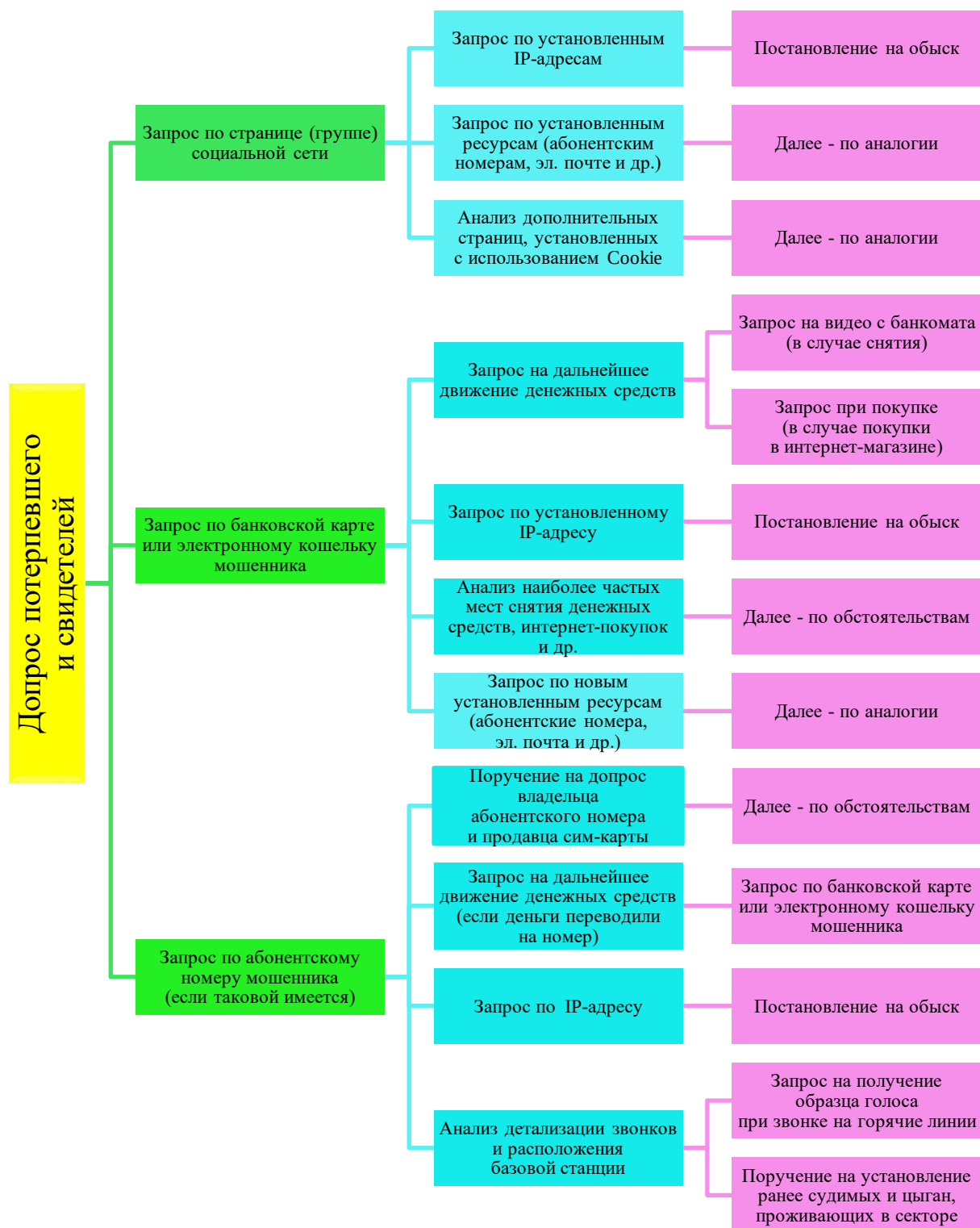


Рис. 34. Порядок действий сотрудника органов внутренних дел при раскрытии мошенничества, совершенного в современном информационном пространстве в сети Интернет с использованием различных мессенджеров

Мошенничество, совершенное в современном информационном пространстве в сети Интернет с использованием искусственного интеллекта

В 2024 году на Алтае был зарегистрирован первый в истории случай мошенничества с помощью искусственного интеллекта. Злоумышленники, подделав голос и видео жительницы города Барнаула, смогли украсть деньги ее знакомых, используя фразу: «Мне просто оплату сейчас сделать нужно, а у меня карта на сутки заблокирована, если что, я завтра к обеду смогу вернуть».

Такие сообщения получили десятки контактов жителей Барнаула от имени Марины Василенко. Это ее голос. Хотя девушка ничего не отправляла. Пять человек откликнулись на просьбу. На неизвестную карту жители отправили более 100 тыс. руб. По словам Марины Василенко, первой позвонила ее подруга и сообщила: «Я тебе отправила деньги. Ты получила их?» Марина поняла, что мошенники взломали ее Telegram-аккаунт. Используя видео и голосовые сообщения Марины Василенко, оставленные ранее в различных мессенджерах, с помощью искусственного интеллекта мошенники создали новые, с нужным им текстом. Давние друзья и родственники ничего не заподозрили, услышав знакомый голос, да еще и получив видео-сообщение от девушки. Марина написала заявление в полицию. Это первый в истории случай мошенничества с использованием нейросетей. Раньше, чтобы подделать голос и создать дипфейк, то есть портрет человека с чужим лицом, потребовалось бы несколько дней, сегодня это займет не больше минуты, причем распознать человека и лжесообщение практически невозможно. Все упирается только в два параметра. Если у злоумышленника есть время и деньги, можно сделать любой дипфейк, который пройдет почти любые проверки. Недолгий поиск нейросети в Интернете, обычная фотография, скаченная из социальных сетей человека, и несколько минут ожидания.

В подобных случаях необходимо перезвонить абоненту, от имени которого ведется разговор, если же возможности позвонить нет, – задать личный вопрос в сообщении, ответ на который знает потерпевший и тот, кто обращается с просьбой о заёме денежных средств. Поможет звонок человеку, от имени которого просят занять денежную сумму. Далее необходимо проверить видео-сообщение на предмет монотонной речи собеседника, неестественной мимики. Нужно быть бдительным при получении обычных текстовых сообщений. Эти схемы давно уже всем известны, но, к сожалению, в современном информационном пространстве хорошо работают. В 2024 году жители Алтайского края действиями мошенников в сфере информационно-коммуникационных технологий от такого вида мошенничества потеряли свыше млрд руб. (канал ТВ «РОССИЯ-1» от 30 сентября 2024 г.) (см. рис. 35).

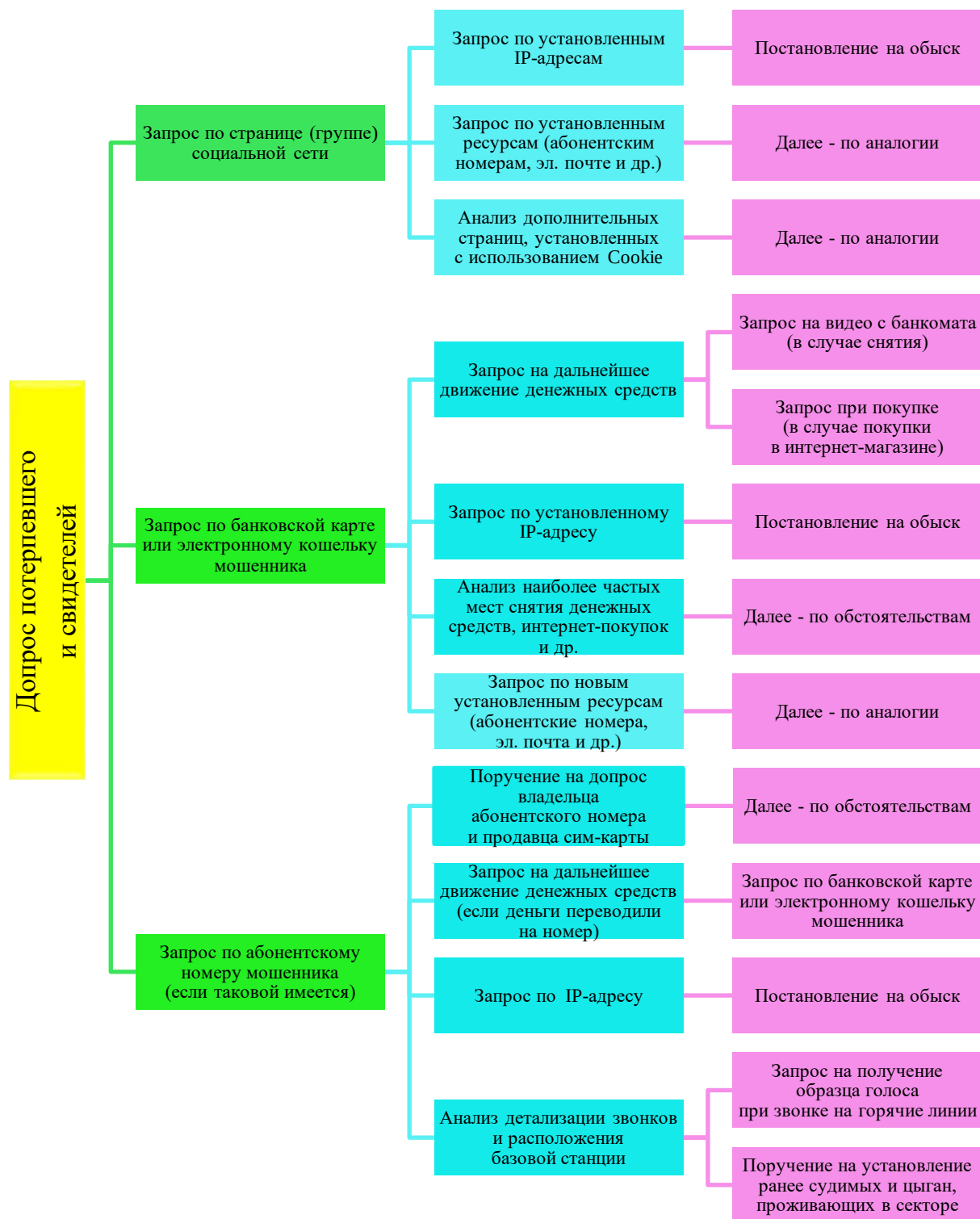


Рис. 35. Порядок действий сотрудника органов внутренних дел при раскрытии мошенничества, совершенного в современном информационном пространстве с использованием искусственного интеллекта

Мошенничество, совершенное в современном информационном пространстве в сети Интернет с использованием QR-кода

В настоящее время преступники стали использовать новый вид такого мошенничества, как сканирование QR-кода. При этом законопослушные граждане, используя современные виды платежей в торговых сетях и иных общественных местах, в целях экономия времени часто осуществляют взаиморасчет с использованием предоставляемого отсканированного QR-кода.

Покупатели и другие граждане не подозревают, что данный вид платежа может предоставить доступ к их личным данным. В предоставленный QR-код мошенники заранее внедряют вредоносную программу, при помощи которой они получают доступ к управлению не только денежными средствами пользователя, но и к другой, принадлежащей ему личной цифровой информации.

За доли секунды телефон может загрузить вредоносную программу, предоставляя преступнику доступ к личным данным, сообщениям, контактам, микрофону, камере и даже местоположению. QR-код (англ. *Quick Response code* – «код быстрого отклика») – тип привычного штрих-кода, но он может содержать гораздо большую информацию по сравнению с предыдущей версией. При сканировании QR-кода он быстро расшифровывает информацию. Телефон на автомате выполняет любое действие, закодированное в шаблоне, например открыть сайт, загрузить приложение и отправить платеж. Это хитрый способ обойти защиту телефона (мобильного устройства), так как пользователь добровольно отсканировал код и открыл мошеннику «дверь». Пагубность заключается в отсутствии у пользователя подозрений, что в его мобильное устройство заложена вредоносная программа.

При сканировании QR-кода может возникнуть и другая ситуация. В нашей повседневной жизни мы часто прибегаем к фотографии и хотим запечатлеть важные события, однако при фотографировании мы можем случайно захватить вредоносный QR-код, размещенный мошенником заранее на том или ином стенде, стене, фотообоях и т. д.

Чтобы не попасться на уловку злоумышленников, необходимо правильно оценить возникшую жизненную ситуацию и лучше всего не использовать QR-код (см. рис. 36).

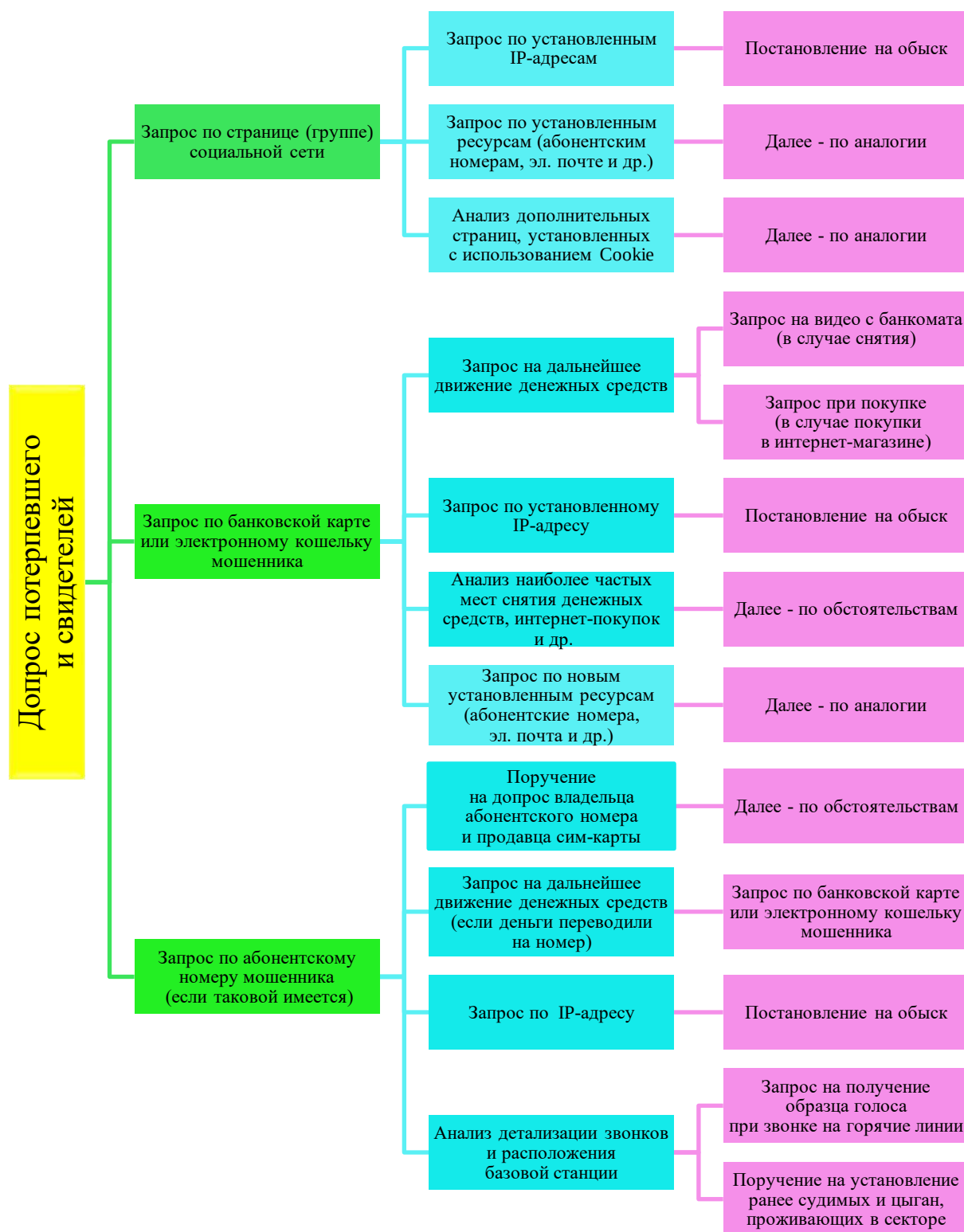


Рис. 36. Порядок действий сотрудника органа внутренних дел при раскрытии мошенничества, совершенного в современном информационном пространстве в сети Интернет с использованием QR-кода

**Раскрытие преступления,
связанного с получением крупной взятки в криптовалюте
с использованием современного информационного пространства
в сети Интернет**

Балашихинский городской суд вынес приговор по делу о получении следователем крупной взятки в криптовалюте. На скамье подсудимых оказался бывший руководитель следственного отдела СКР по Тверскому району г. Москвы Марат Тамбиев. Его обвиняли в получении крупнейшей в истории России взятки – больше 7 млрд руб. Несколько лет назад в производстве бывшей подчиненной М. Тамбиева следователя Кристины Лиховенко находилось уголовное дело в отношении группировки хакеров.

Преступники организовали в Даркнете, по сути, маркетплейс по торговле личными данными. Организованная преступная группа располагала большими денежными средствами. Узнав об этом, М. Тамбиев, по версии обвинения, вступил в преступный сговор с членами организованной преступной группы и начал с ними вести торги. Предложил киберферистам меру пресечения в виде «домашнего ареста» вместо нахождения в СИЗО. За данную услугу злоумышленники щедро отблагодарили М. Тамбиева, а именно: передали М. Тамбиеву пароли от криптокошельков, на которых хранились миллиарды. С целью недопущения разоблачения должностного преступления в получении взятки бывший следователь М. Тамбиев хранил данную информацию в ноутбуке в папке под названием «Пенсия».

После совершения сделки между начальником следственного отдела и членами организованной преступной группы хакеры сообщили о совершенном должностном преступлении М. Тамбиевым сотрудникам ФСБ России. В результате полученной оперативно значимой информации в отношении М. Тамбиева были проведены оперативно-розыскные мероприятия. В процессе наблюдения за М. Тамбиевым выяснилось, что он часто посещал «Кальянную» в центре г. Москвы. В процессе документирования его преступной деятельности было установлено получение взятки в особо крупном размере в виде криптовалюты. Тамбиева М. задержали с поличным в момент получения очередной взятки от адвоката хакеров. В процессе документирования преступной деятельности М. Тамбиева было установлено, что он действовал не один, а со своей подчиненной К. Лиховенко, с которой успел поделиться своим миллиардным состоянием. Следователи сумели доказать как минимум десять эпизодов получения взяток. Нажитое преступным путем – квартиры,

машины, мотоцикл – конфискованы в доход государства по решению суда. Во время расследования уголовного дела миллиарды биткоинов, находившихся в интернет-пространстве, официально обратили в доход государства.

Бывшего следователя К. Лиховенко приговорили к 9 годам лишения свободы, а начальник следственного отдела СКР по Тверскому району г. Москвы М. Тамбиев осужден к 16 годам лишения свободы с отбыванием срока наказания в колонии строгого режима, с назначением штрафа в 500 млн руб. и обязанностью вернуть государству 7 млрд руб. (см. рис. 37).

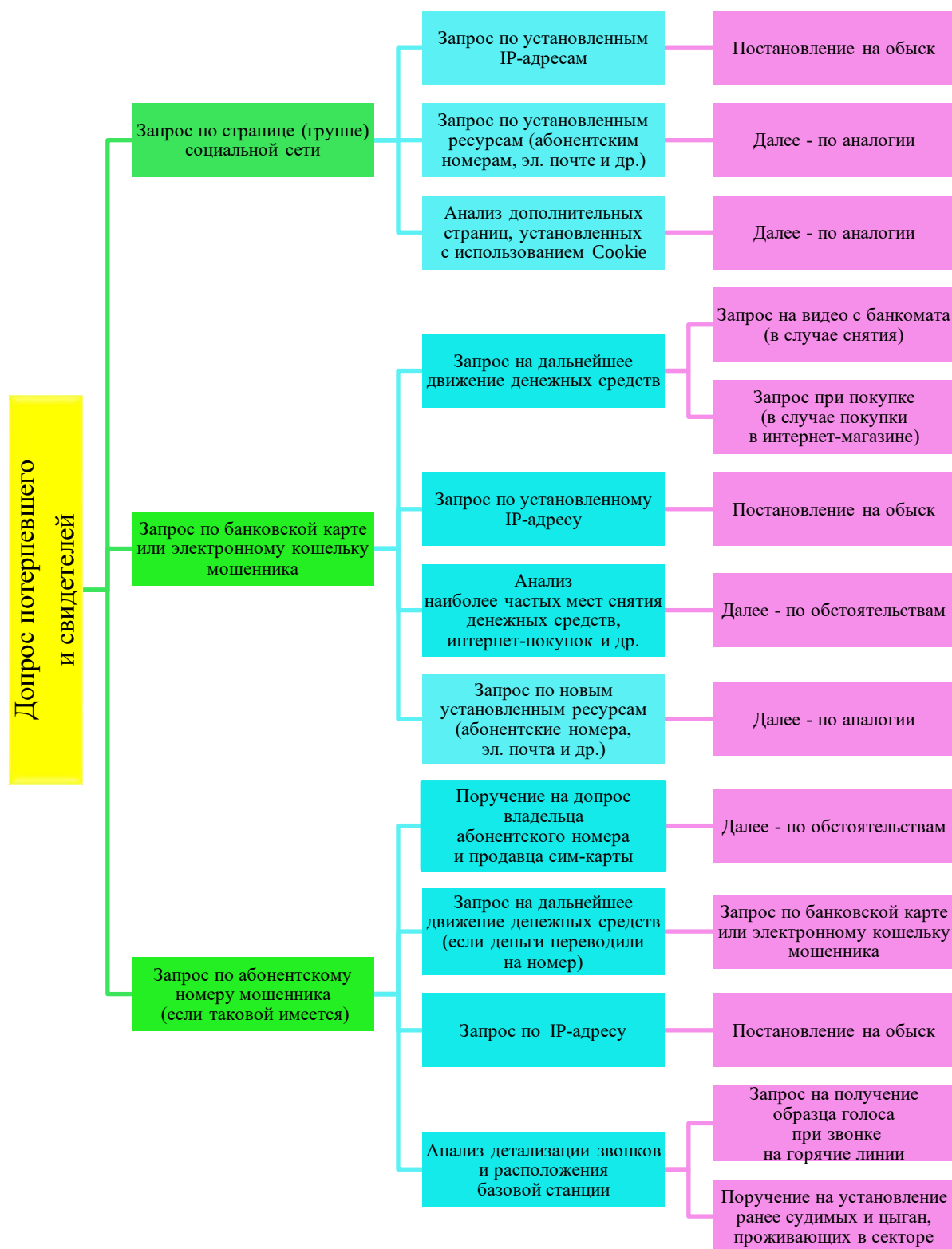


Рис. 37. Порядок действий сотрудника органов внутренних дел при раскрытии преступлений, связанных с криптовалютой, в современном информационном пространстве с использованием сети Интернет

**Раскрытие преступления в сфере медицины,
совершенного в современном информационном пространстве
с использованием сети Интернет организованной преступной группой**

В Москве обезвредили организованную преступную группу, совершавшую мошеннические действия с целью оказания медицинской помощи. В результате полученной оперативно значимой информации о данных преступных деяниях был намечен план оперативно-розыскных мероприятий, проводимых в тесном взаимодействии сотрудников ФСБ России и МВД России. В процессе документирования преступной деятельности была установлена роль каждого участника, а результаты собранного материала послужили основой для задержания подозреваемых.

Как выяснилось, аферисты пользовались лицензией на оказание частной медицинской помощи на дому, а свои услуги они рекламировали в современном информационном пространстве с использованием сети Интернет. На улице Смирновской они незаконно открыли псевдополиклинику и реабилитационный центр, куда отправляли пациентов, страдающих алкогольной и наркотической зависимостью. После госпитализации пациентов в лжемедицинское учреждение их родственникам сообщали, что больные находятся в крайне тяжелом состоянии и им необходимо срочное дорогостоящее лечение. Поверив мошенникам, граждане переводили денежные средства на банковские счета, указанные мошенниками. По предварительным подсчетам, общий ущерб превышал миллионы рублей. По данным фактам возбуждено восемь уголовных дел по статье «Мошенничество». В результате отлаженного взаимодействия ФСБ России и МВД России все члены организованной преступной группы задержаны (см. рис. 38).

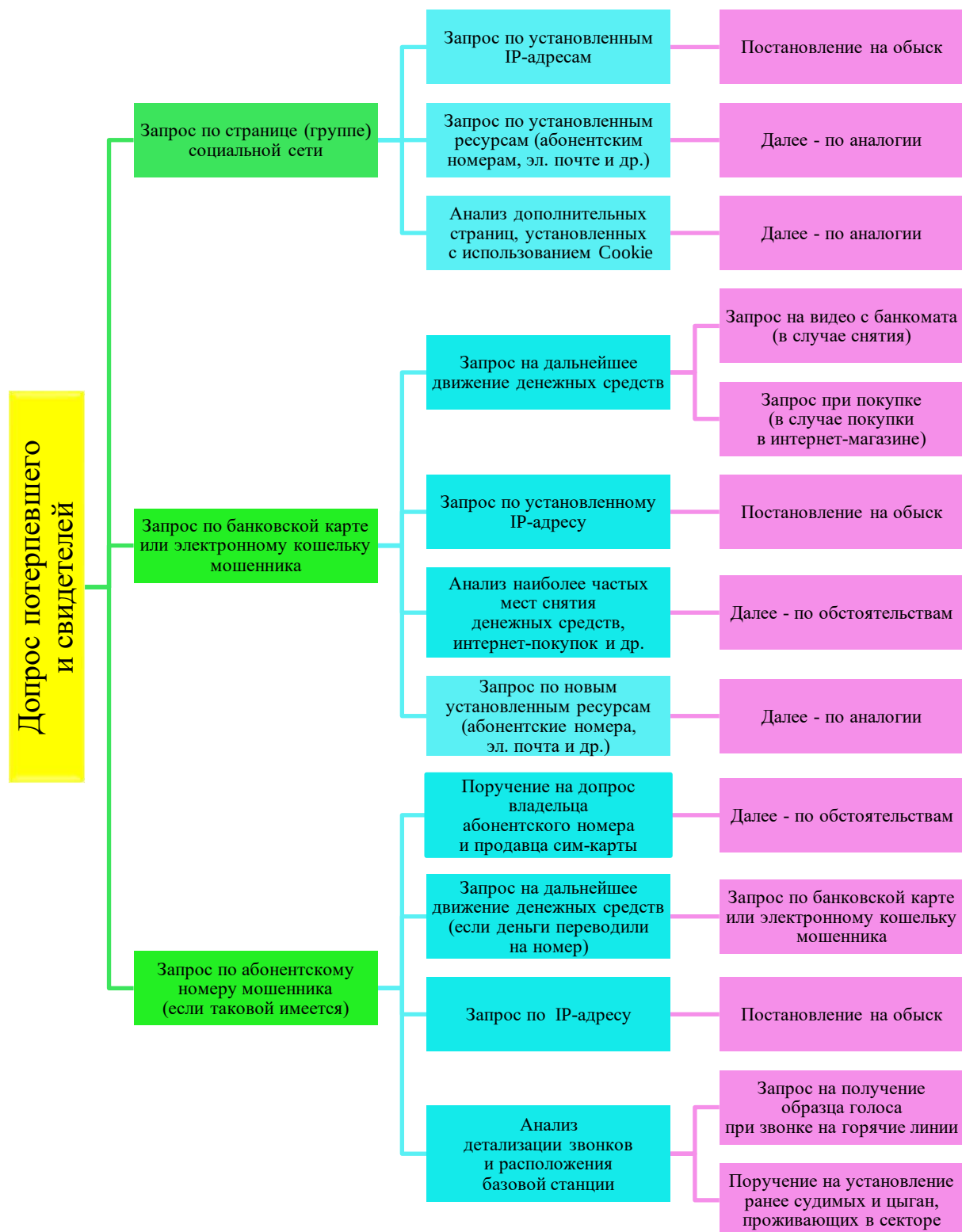


Рис. 38. Порядок действий сотрудника органов внутренних дел при раскрытии преступлений, связанных со сферой медицины, в современном информационном пространстве с использованием сети Интернет

**Предотвращение попыток совершения актов терроризма,
подготовленных украинскими спецслужбами
в современном информационном пространстве
с использованием сети Интернет**

С начала проведения специальной военной операции сотрудники СБУ активно используют возможности современного информационного пространства. Через социальные сети они ведут поиск лиц, враждебно настроенных и не согласных с политикой, проводимой руководством Российской Федерации. Устанавливая таких граждан, сотрудники спецслужб Украины через социальные сети проводят с ними психологическую обработку, направленную на последующее осуществление вербовочных манипуляций с целью дальнейшего их использования для совершения преступлений экстремистской направленности и террористического характера.

Так, в *Ярославской области* сотрудниками ФСБ России предотвращен террористический акт, планируемый на одном из оборонных предприятий. Задержан гражданин России, которого ранее завербовали через мессенджер «Telegram». Он получил от заказчиков предполагаемого преступления мешок с токсичным веществом, используя который, должен был отравить сотрудников военного завода. Преступник был задержан с поличным. На допросе он дал показания о том, что в социальных сетях выражал свое недовольство проведением СВО, в связи с чем в декабре 2024 г. в мессенджере «Telegram» на него вышел представитель Украины под ником «великий воин корпуса», предложивший за денежное вознаграждение совершить террористический акт. Мужчина, по указанию своих украинских кураторов, должен был залить в воздухопроводы машин, принадлежащих работникам оборонного предприятия Ярославской области, ядовитую жидкость. Сначала им была проведена рекогносцировка местности, автопарковки, полученные сведения он отправил своему куратору, за что получил 10 тыс. руб. В последующем ему прислали мешок с ядовитым веществом, указав координаты тайника через социальные сети. После задержания данного гражданина изъятый мешок с ядовитым веществом был отправлен на соответствующее исследование, установившее что попадание паров данного яда в верхние дыхательные пути человека может произвести острый ожог слизистой с возможным развитием асфиксии с летальным исходом. При попадании на кожу могут возникать острые ожоги, язвы или рубцы.

В *Ростове-на-Дону* суд рассмотрел уголовное дело в отношении уроженца Мелитополя Егора Семенова, который свою вину полностью признал. На видеозаписи отчетливо видно, как он покупает напитки, в которые позже нальет отраву. К спиртному прилагался еще и торт. Е. Семенов сам доставил отравленные напитки и торт в ресторан, где летчики отмечали 20-летие выпуска из Армавирского высшего военного авиационного училища, якобы от сослуживца, который не смог приехать. Собравшиеся на праздник успели только разрезать торт, дальше сработала интуиция, и все, что привез странный курьер, направили на экспертизу. За массовые убийства российских офицеров киевские наниматели пообещали Е. Семенову 400 тыс. руб., но денег он так и не получил.

Еще один пример подготовки террористического акта в современном информационном пространстве с использованием сети Интернет. В *Санкт-Петербурге* завербованные главным управлением разведки Украины граждане планировали отправить на фронт посылку с отравленными крупами, кашами, зерном, мукой, сахаром, растворимым кофе. После добавления яда преступники искусно запечатывали упаковки в подпольной лаборатории. Оказавшись в зоне СВО, все это попало бы не только на столы военнослужащих, но и мирного населения. У организаторов преступлений была одна цель – уничтожить как можно больше населения Российского государства. Сотрудниками ФСБ России своевременно была получена оперативно значимая информация, которая в результате отработки способствовала предотвращению террористических актов. В процессе проведения оперативно-розыскных мероприятий был установлен гараж, где располагалась подпольная лаборатория и осуществлялась преступная деятельность в виде производства ядохимикатов для последующего их использования в целях совершения террористических актов на территории Российской Федерации. В данном гараже при производстве обыска обнаружено более 20 кг ядовитого вещества.

Таким образом, спецслужбами Украины в тесном взаимодействии со службами стран северо-западного альянса избрана тактика «неизбирательных убийств множества случайных людей» способом использования отравляющих веществ, производство которых ведется в западных странах. Достаточно вспомнить, как сотрудниками ФСБ России в феврале 2024 г. предотвращен террористический акт в Запорожье при изъятии у граждан Украины препаратов, разработанных в США,

применяющихся для создания химического оружия. С точки зрения спецслужб Украины, это абсолютно «нормальные» методы борьбы с врагом.

Сотрудники СБУ и других стран северо-западного альянса потенциального убийцу тщательно подвергают психологической обработке, практически его зомбируют и превращают в послушного «робота», действующего по команде и выполняющего любое поручение без раздумий. Украинские спецслужбы занимаются подбором граждан – будущих жертв, имеющих ненавистнические взгляды по отношению к России, заинтересовывают людей материальной составляющей. Финал между тем для всех граждан, завербованных спецслужбами СБУ и стран западного альянса, один – после выполнения части задуманного преступного задания или совершения преступления исполнителей ликвидируют. Только по ст. 205 УК РФ «Терроризм» преступнику грозит лишение свободы на срок до 20 лет, а если рассматривать ситуацию как в случае с армавирским отравителем, где предъявлено обвинение как в теракте (п. «а» ч. 3 ст. 205 УК РФ), так и в государственной измене (ст. 275 УК РФ), то и вовсе грозит пожизненное заключение (см. рис. 39).

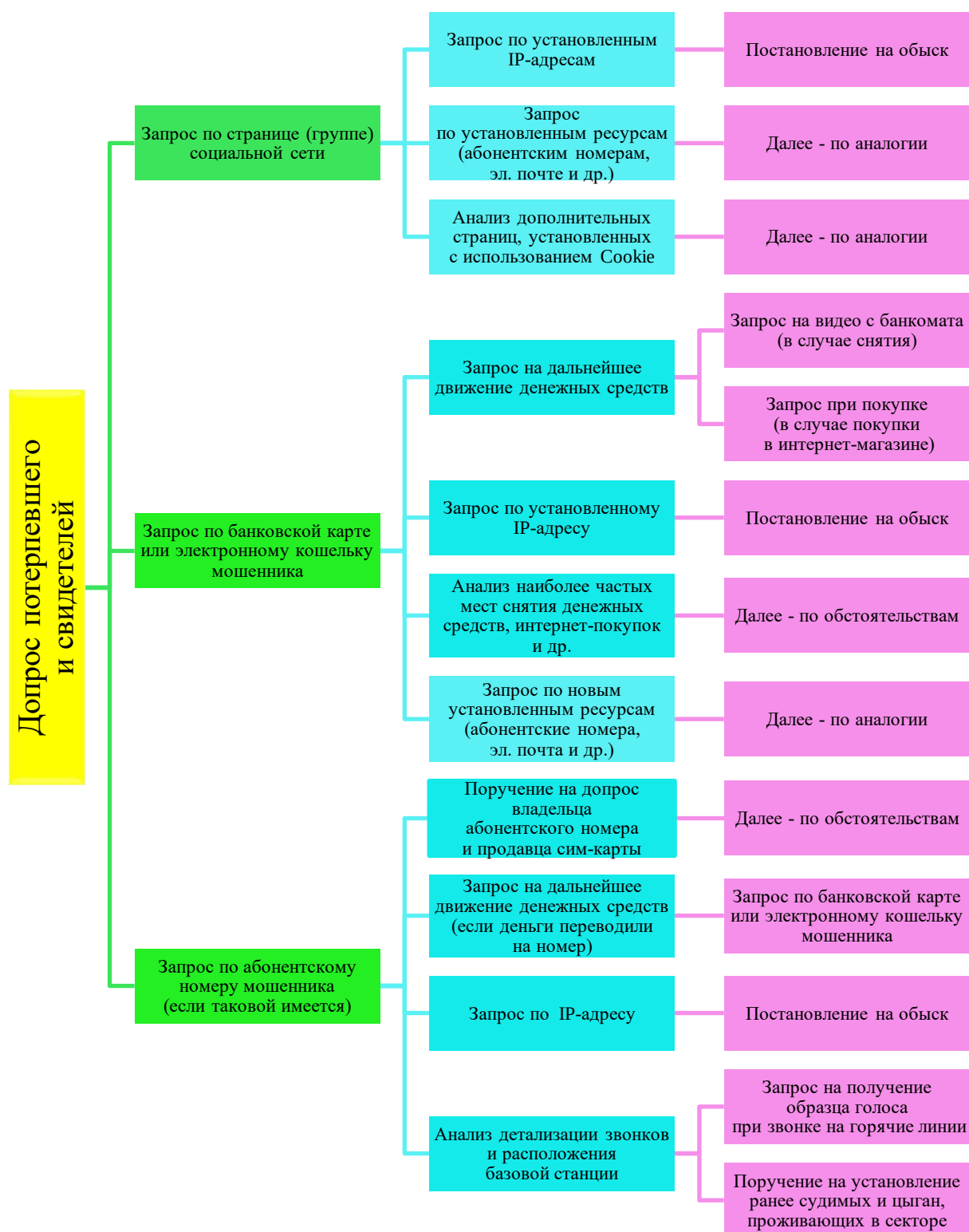


Рис. 39. Порядок действий сотрудника органа внутренних дел при предотвращении попыток совершения актов терроризма, подготовленных украинскими спецслужбами в современном информационном пространстве с использованием сети Интернет

Раскрытие преступлений, совершенных кибермошенниками в современном информационном пространстве с использованием сети Интернет и новых методов обмана

Раскрывая тему данного вопроса, авторы проанализировали ситуации, складывающиеся между мошенниками и потерпевшими, и в целом криминогенную обстановку. Лишь после этого нами был сделан вывод о том, что не всегда необходимо верить содержанию информации, поступающей по телефону от родственников, друзей и даже близких людей. Любую информацию следует подвергать тщательному анализу, так как в условиях больших возможностей IT-технологий кибермошенники легко могут при помощи искусственного интеллекта создать голос родственника, друга или близкого человека.

В одном из своих интервью, посвященном новым методам обмана, которые используют кибермошенники, вице-премьер Правительства Российской Федерации Дмитрий Григоренко обсудил подробности с обозревателем Наилей Аскер-заде³¹. Ключевой фразой было то, что кибермошенники для осуществления своих преступных целей идут на любые уловки, чтобы выманить деньги у доверчивых граждан. По мнению Дмитрия Григоренко, в настоящее время не стоит доверять даже близким родственникам. С помощью современных информационных технологий мошенники подделывают голоса родных и близких. Абонент слышит голос не мошенника, а поддельный голос родного (близкого) человека, которому доверяет. Абсолютно не сложно сделать фейк – подделать голос любого человека, главное – записать оригинальный голос. После этого мошенники пытаются узнать пароль к личному кабинету в банке либо к госуслугам, а потом пробуют оформить кредиты. В таких внезапно возникших ситуациях Дмитрий Григоренко рекомендует: прежде чем делиться конфиденциальными данными, все же необходимо перезвонить родственникам на их личные номера и уточнить информацию.

После выявленных многократных вышеназванных мошеннических манипуляций, направленных на завладение конфиденциальной информацией, и последующих денежных хищений Правительство Российской Федерации приняло ряд законопроектов, одним из которых является законодательный запрет на звонки госучреждений и госорганов, маркет-плейсов, банков через мессенжеры. В этом году такая норма прописана на законодательном уровне.

³¹ Новостная лента телевизионного канала «РОССИЯ-1» от 26 февраля 2025 г.

Кроме того, государство обязало маркировать все звонки, которые осуществляются от имени организаций, банков, госучреждений, медицинских учреждений. В этом случае у абонентов будет высвечиваться не номер телефона цифрами, а название организации. Естественно, если происходит звонок от неизвестного абонента, т. е. высвечивается цифрами неизвестный номер телефона, то в таком случае лицо, которому звонят, должно понимать, что, вероятнее всего, ему звонит мошенник.

В качестве предупредительной меры используется установка определенного временного интервала (тайминга) на получение нового пароля в случае его изменения на госуслугах. У большинства граждан на сервисе существует двухфакторная аутентификация. При смене пароля необходимо направлять подтверждение через смс-сообщение. Второе сообщение будет приходить с интервалом 10–15 минут, чтобы было время для обдумывания и понимания происходящего.

К нашему сожалению, объемы хищений пока только растут. В прошлом году рост превысил 74 %. Мошенники похитили со счетов россиян 27,5 млрд руб. Это рекордный показатель за все время ведения статистики. Размер возмещения причиненного материального вреда законопослушным пользователям ничтожно мал – менее 10 %.

Далее Дмитрий Григоренко пояснил, что за последние годы в Российской Федерации использование интернет-трафика выросло на 20–30 %. Сегодня 85 % территории страны обеспечено доступом к Интернету. В среднем мировой показатель использования интернет-трафика составляет 65–70 %. По итогам прошлого года наша страна заняла 12-е место по цене фиксированного Интернета среди 223 стран (см. рис. 40).

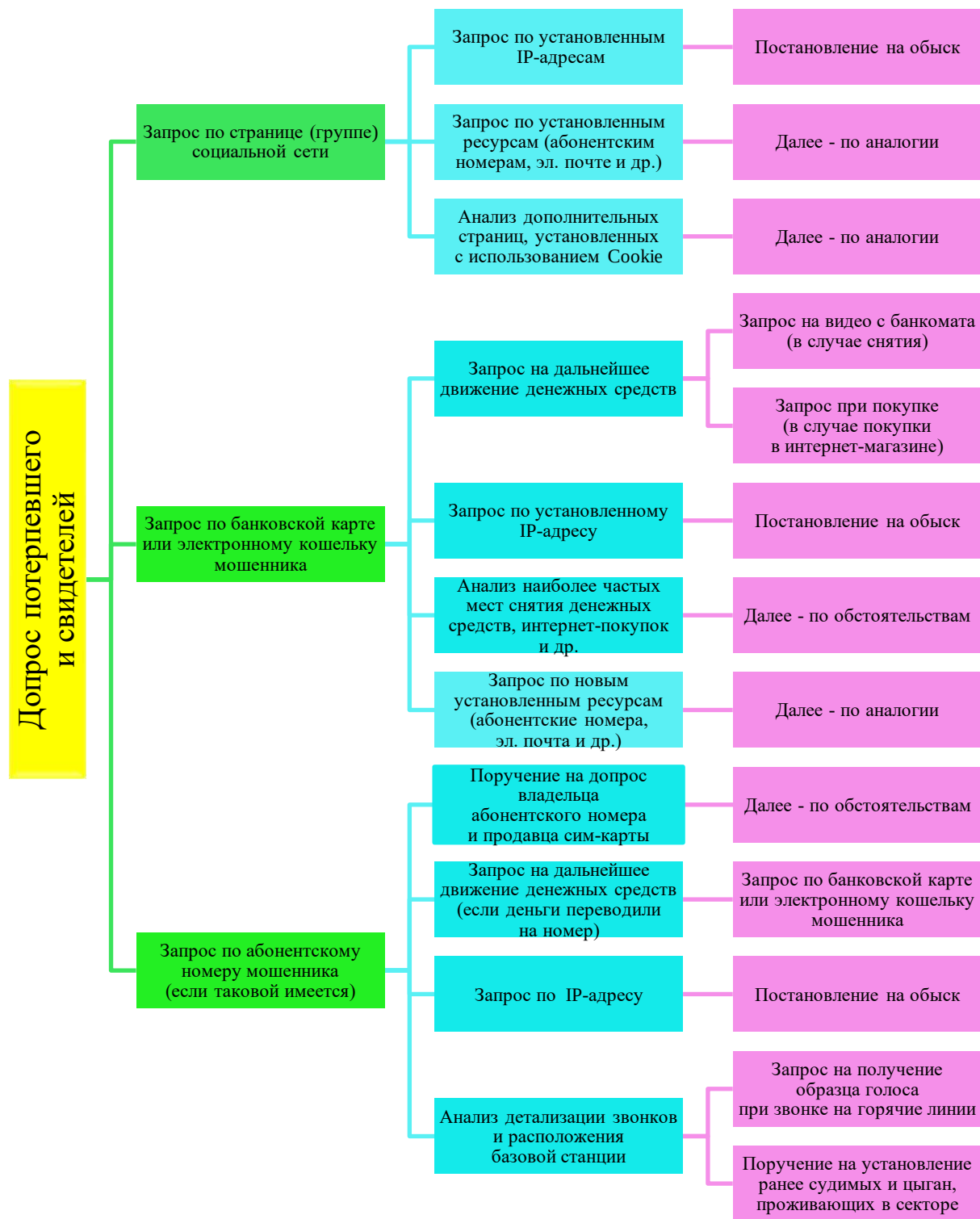


Рис. 40. *Раскрытие преступлений, совершенных кибермошенниками в современном информационном пространстве с использованием сети Интернет и новых методов обмана*

Глава 4.

Роль сотрудников оперативных подразделений органов внутренних дел Российской Федерации в раскрытии преступлений, совершаемых в современном информационном пространстве с использованием сети Интернет

В число оперативных подразделений, функциональные обязанности которых определяют раскрытие преступлений, совершаемых в современном информационном пространстве с использованием сети Интернет, входят: Главное управление уголовного розыска Министерства внутренних дел Российской Федерации (ГУУР МВД России), Управление по организации борьбы с противоправным использованием информационно-коммуникационных технологий Министерства внутренних дел Российской Федерации (УБК МВД России), Управление экономической безопасности и противодействия коррупции Министерства внутренних дел Российской Федерации (УБЭПК МВД России), Главное управление по противодействию экстремизму Министерства внутренних дел Российской Федерации (ГУПЭ МВД России)³².

Не умаляя достоинства ни одного из перечисленных подразделений, все-таки хотим остановиться на одном из них, так как даже во времена революции в царской России существовал уголовный сыск, который затем уже был переименован в уголовный розыск, и большинство совершаемых преступлений раскрывалось именно сотрудниками уголовного розыска. Безусловно, история становления Российского государства с течением временных этапов проходит необходимые жизненно важные пути, и в связи с этими преодолениями наше современное общество меняется в лучшую сторону, обогащая каждого гражданина в широком понимании этого значения. Общение людей между собой становится несколько иным: переход от бумажных писем и проводных телефонов к развивающимся ИТ-технологиям, использование возможностей современного информационного пространства, в том числе и сети Интернет. Вместе с тем возможностями информационно-коммуникационных технологий интересуются и лица, склонные к незаконному обогащению посредством их использования. Тенденция такова, что помимо преступных элементов, некоторые граждане, получив

³² Об утверждении Перечня оперативных подразделений органов внутренних дел Российской Федерации, правомочных осуществлять оперативно-розыскную деятельность: приказ МВД России от 31 марта 2023 г. № 199 // Информационно-правовой портал «Гарант.Ру». – URL: <https://www.garant.ru/products/ipo/prime/doc/407440201/> (дата обращения: 10.09.2025).

высшее образование и не определившись в социуме, используют свои специальные знания в целях совершения преступлений в сети Интернет. В связи с этим функциональные обязанности сотрудников уголовного розыска пересматриваются и расширяются, одним из таких направлений является раскрытие преступлений в современном информационном пространстве с использованием сети Интернет.

4.1. Исторический аспект оперативно-служебной деятельности Московского уголовного розыска ГУ МВД России по г. Москве

Сотрудники Московского уголовного розыска с достоинством и честью проходят свой нелегкий путь, который насчитывает уже более ста лет.

После изучения международного опыта полицейской работы многих зарубежных стран, у которых есть много интересных наработок и передовых технологий, начальник ГУ МВД России по г. Москве генерал-лейтенант полиции О. А. Баранов, посвятивший большую часть своей служебной деятельности уголовному розыску, закономерно сделал вывод: «Московский уголовный розыск – лучший в мире».

Генерал-лейтенант полиции О. А. Баранов искренне убеждён, что методика раскрытия преступлений, применяемая российскими правоохранительными органами, результаты работы сыскных аппаратов существенно отличаются от того, что удаётся их зарубежным коллегам. Особенно это заметно в решении проблемы борьбы с организованной преступностью. Поэтому не зря сотрудников Московского уголовного розыска, выезжающих за рубеж для обмена опытом, после их выступлений на всякого рода семинарах и конференциях долго не отпускают с трибуны, засыпая бесконечными вопросами.

Секрет профессионализма российских сыщиков, их целеустремлённости в достижении цели и в конечном итоге результативности работы во многом зависит от методики подбора, обучения и воспитания кадров. Как правило, в полицию принимают молодых людей, отслуживших срочную службу в армии. Предпочтение отдаётся бывшим пограничникам, десантникам и спецназовцам, получившим хорошую закалку и сдавшим экзамен на право называться настоящими «мужчинами-воинами».

Новые времена порождают новые проблемы. Большую тревогу у генерал-лейтенанта полиции О. А. Баранова вызывает рост преступлений в сфере информационно-коммуникационных технологий, статистика которых оставляет желать лучшего. Количество преступлений, совершаемых в современном информационном пространстве с использованием сети Интернет с каждым днем увеличивается. Хакерские атаки, которым подвергаются коммуникационные системы правительственных учреждений, в том

числе и МВД России, требуют новых методов защиты информации, выявления и идентификации злоумышленников.

Большие риски несёт с собой внедрение в нашей стране криптовалюты биткойн с использованием сети блокчейн, где контроль со стороны правительственных или финансовых институтов полностью отсутствует. Если для законопослушного делового международного сообщества биткойн и блокчейн – это активы и комфортное средство транзакций, то для недобросовестных предпринимателей и организованной преступности криптовалюта и система её перевода служат способом незаконного вывода денег за рубеж, платежа и обналичивания «грязных денег». В настоящее время мировой оборот биткойнов достиг 12 млрд долл. США, из них 3 млрд составляет преступный оборот.

В то же время криминалитет не стоит на месте. Уже родилась теневая криптовалюта Dash, предназначенная, по словам её создателей, «для свободных, презирающих государство людей», у этой криптовалюты преимущество перед биткойном в том, что её транзакция осуществляется за 15–20 секунд, в то время как биткойну на это потребуется 5–10 минут. В европейских странах и на постсоветском пространстве преступный мир получил ещё одну криптовалюту Zcash. В США и в странах Латинской Америки криминалитет использует криптовалюту Monero.

Люди, продвигающие криптовалюту, пытаются убедить правоохранителей в том, что способом борьбы с хищением бюджетных средств в компьютерных сетях может служить сама система блокчейн, поскольку она представляет собой большую бухгалтерскую книгу, в которой сохраняется информация обо всех транзакциях и их участниках. Поэтому следовательно ничего не нужно искать и доказывать, так как за него всё сделают программный код и архивы с памятью. А в заключение они делают вывод: повсеместное внедрение блокчейн – идеальный способ борьбы с коррупцией и «беловоротничковой преступностью». Может быть, считает О. А. Баранов, когда-нибудь так оно и будет, но на сегодняшний день блокчейн является инструментом в руках криминального интернационала по отмыванию «грязных денег». И вообще, кибернетическая преступность, совершая преступления в современном информационном пространстве с использованием сети Интернет, приобрела в мире такой объём, что начала представлять серьёзную угрозу национальной безопасности. В настоящее время может возникнуть такая ситуация, когда за стенкой, в соседнем подъезде может проживать хакер, который, зарегистрировавшись в дальнем зарубежье, с помощью технических средств занимается вымогательством у соседей по дому или взламывает защитную систему банка. Вычислить такого умельца можно, но только с помощью не менее продвинутого специалиста.

Большие надежды на успех в борьбе с преступлениями в сфере информационных технологий О. А. Баранов возлагает на молодое поколение, обучающееся в настоящее время в учебных заведениях МВД России и обладающее высокоразвитым техническим мышлением. При правильном воспитании в лучших традициях Московского уголовного розыска и созданного Управления по борьбе с противоправным использованием информационно-коммуникационных технологий они могут стать той силой, которой будет по плечу бороться с самыми продвинутыми киберпреступниками.

В одном из интервью генерал-лейтенант полиции О. А. Баранов высказал свою точку зрения о том, что столичная полиция слишком часто отвлекается от выполнения своих основных функциональных обязанностей на предотвращение нежелательных эксцессов во время проведения несанкционированных митингов, шествий и демонстраций, инициаторами которых выступают всякого рода провокаторы, называющие себя оппозиционерами, которые выманивают людей на улицы, действуют либо в угоду врагам России или исключительно в своих собственных корыстных интересах.

На одном из брифингов О. А. Баранова спросили: «Вы действительно считаете, что российский уголовный розыск лучший в мире? Ведь всегда и везде в пример ставили лондонский Скотленд Ярд». Ответ был прост и доходчив: «Да, именно так считаю, и вот почему. Ни одна уголовная полиция в мире не сталкивалась с такими вызовами и не решала таких проблем и в таком объёме, как наша. Нигде в мире нет такой товарищеской спайки оперативных работников, как в МУРе. А что до известности Скотленд Ярда, то он её получил исключительно благодаря литературным произведениям писателей XIX столетия и начала XX столетия, но описанные в них успехи – мнимые, в действительности всё гораздо скромнее. Как-то к нам в МУР приехали английские детективы, и я поинтересовался, бывали ли они в музее Шерлока Холмса на Бейкер Стрит? И был удивлён, когда выяснилось, что они никогда даже не слышали о существовании такого музея, а о самом Шерлоке Холмсе, оказывается, узнали лишь из нашего фильма, который демонстрировался по английскому телевидению»³³.

³³ Уголовный сыск в России лучший в мире // Еженедельная газета «Петровка, 38: [сайт]. – URL: <https://petrovka-38.com/arkhiv/item/ugolovnyj-sysk-rossii-luchshij-v-mire> (дата обращения: 21.12.2025).

4.2. Анализ организации оперативно-служебной деятельности УУР и УБК ГУ МВД России по г. Москве при раскрытии преступлений, совершенных в современном информационном пространстве с использованием сети Интернет

Рассматривая научно-исследовательский сегмент данной тематики, считаем необходимым привести некоторые примеры по раскрытию преступлений, совершаемых в современном информационном пространстве с использованием сети Интернет, где оперативно-розыскная деятельность осуществлялась на высоко профессиональном уровне сотрудниками управления уголовного розыска и управления по борьбе с киберпреступлениями ГУ МВД России по г. Москве.

По итогам 2023 года регистрация общеуголовных дистанционных хищений в г. Москве выросла с 39 611 до 47 769 (на 20,6 %). Значительный рост обусловлен снижением регистрации таких преступлений в 2022 году (в связи с началом СВО и переездом мошеннических колл-центров на территорию западной части Украины). В сравнении с аналогичным периодом 2021 года (46 710) количество зарегистрированных дистанционных хищений общеуголовной направленности увеличилось всего на 1 059 преступлений (2,2 %).

Очевидна тенденция по увеличению ущерба от действия преступников – около 33 млрд руб. (АППГ – 23 млрд руб.). Действия преступников становятся все более профессиональными, централизованными, с четким распределением ролей, использованием новейших технологий: «холодные звонки», «автоматические сервисы» по переводу денежных средств, добытых преступным путем.

Необходимо отметить, что в 2023 году доля совершенных преступлений в отношении лиц пожилого возраста в общей структуре увеличилась на 83,4 % (2022 год – 7 100, 2023 год – 13 023). Вместе с тем снижается регистрация дистанционных краж – 10 662 (АППГ – 11 769, –1 107, –9,4 %). Данная динамика связана как с задержанием участников организованных групп и преступных сообществ

(далее – ОГиПС), так и с профилактической работой кредитно-финансовых организаций, эволюционирующей антифрод-системой³⁴. Увеличилось количество зарегистрированных мошенничеств – 40 692 (АППГ – 31 261). Данный факт связан с тем, что завладеть сознанием человека

³⁴ *Антифрод* (от англ. *anti-fraud* – «борьба с мошенничеством») – это программно-аппаратный комплекс, направленный на выявление и предотвращение мошеннических операций в финансовой сфере.

в криминальных целях проще, играя на его страхах и сомнениях, чем обойти автоматические системы кредитно-финансовых учреждений.

Несмотря на рост регистрации дистанционных хищений, увеличилось количество предварительно расследованных уголовных дел на 1 304 или 14,0 % (с 9 338 до 10 642), из них совершенных в составе ОГиПС – 4 996 (АППГ – 5 034). Раскрываемость составила 20,4 % (АППГ – 20,0 %).

Сотрудниками службы УР раскрыто 5 645 преступлений, что на 1 394 больше аналогичного периода прошлых лет. В том числе увеличилось количество раскрытых преступлений в составе ОГиПС на 294 или 26,6 % (с 1 104 до 1 398). Кроме того, в два раза увеличилось количество раскрытых преступлений прошлых лет (далее – ППЛ) – с 588 до 1 104.

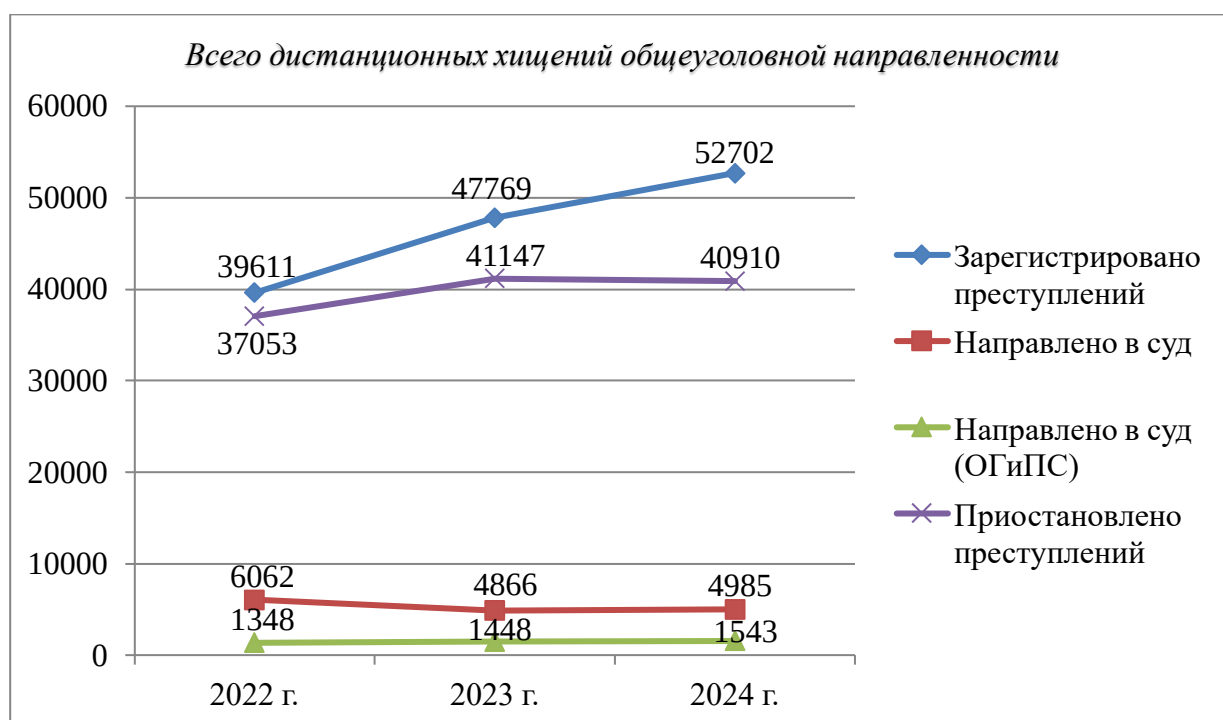


Диаграмма 7. *Количество дистанционных хищений общеуголовной направленности (2022, 2023, 2024 гг.)*

Всего раскрыто службой УР – 5 646 (АППГ – 4 251), ППЛ – 1 104 (АППГ – 588). Всего раскрыто службой УР ОГиПС – 1 398 (АППГ – 1 104), ППЛ – 579 (АППГ – 234). Всего раскрыто ОУР УВД – 1 570 (АППГ – 1 150), ППЛ – 434 (АППГ – 236), ОГиПС – 992 (АППГ – 768), ППЛ – 360 (АППГ – 137). Всего раскрыто 4 отделениями ОУР УВД по АО – 1 134 (АППГ – 529), ППЛ – 313 (АППГ – 178), ОГиПС – 654 (АППГ – 243), ППЛ – 258 (АППГ – 94).

Таблица 1

**Сведения о раскрытии дистанционных преступлений
службой УР (текущий период (ТП) + ППЛ)**

Округ	Всего раскрыто УР (УЧ +ППЛ)	Раскрыто ОГиПС УР	Штат ОУР	Раскрыто ОУР УВД	Нагрузка	Раскрыто ОГиПС ОУР УВД	Нагрузка
ЦАО	1 066	311	180	107	0,66	61	0,37
СВАО	449	152	161	152	0,67	144	1,39
ВАО	423	26	103	34	0,29	16	0,14
ЮВАО	532	156	114	138	1,35	117	1,14
ЮАО	509	74	102	86	0,58	72	0,49
ЮЗАО	712	387	146	321	2,98	298	2,7
ЗАО	867	348	110	587	5,01	323	2,76
СЗАО	488	25	117	92	1,09	3	0,03
САО	881	75	84	140	1,21	28	0,24
ЗелАО	161	45	115	66	1,46	41	0,91
ТиНАО	287	201	45	179	2,55	165	2,35
УВД на ММ	218	92	70	102	5,36	92	4,84

Таблица 2

**Сведения о раскрытии дистанционных преступлений
спецотделами ОУР (текущий период (ТП) + ППЛ)**

Округ	Штат спец отдела	Раскрыто	Нагрузка	Всего раскрыто ОГиПС	Нагрузка	Место
ЦАО	28	40	1,42	13	0,46	10
СВАО	17	17	1	9	0,52	11
ВАО	18	27	1,5	14	0,77	9
ЮВАО	15	115	7,66	114	7,6	4
ЮАО	23	44	1,91	34	1,47	8
ЮЗАО	19	302	15,8	285	15	2
ЗАО	17	510	30	226	13,2	1
СЗАО	12	69	5,75	—	—	7
САО	20	132	6,6	23	1,15	6
ЗелАО	8	45	5,6	36	4,5	5
ТиНАО	12	169	14	158	13,1	3

В 2023 году выявлено три преступных сообщества:

– УУР ГУ МВД России по г. Москве совместно с ОУР УВД по ТиНАО ГУ МВД России по г. Москве в ходе расследования уголовного дела № 12201450137000634, возбужденного по признакам преступления, предусмотренного ч. 4 ст. 159 УК РФ;

– УУР ГУ МВД России по г. Москве совместно с ОУР УВД по СВАО ГУ МВД России по г. Москве в рамках расследования уголовного дела № 12201450025000214, возбужденного по признакам преступления, предусмотренного п. «б» ч. 4 ст. 158 УК РФ;

– ОУР УВД по ЮЗАО ГУ МВД России по г. Москве в рамках уголовного дела № 12301450091000451, возбужденного по признакам преступления, предусмотренного ч. 4 ст. 159 УК РФ.

По итогам 2023 года в суд направлено три уголовных дела по ч. 1 и ч. 2 ст. 210 УК РФ, два из которых раскрыто сотрудниками ОУР УВД по ЮЗАО ГУ МВД России по г. Москве (диагр. 8).

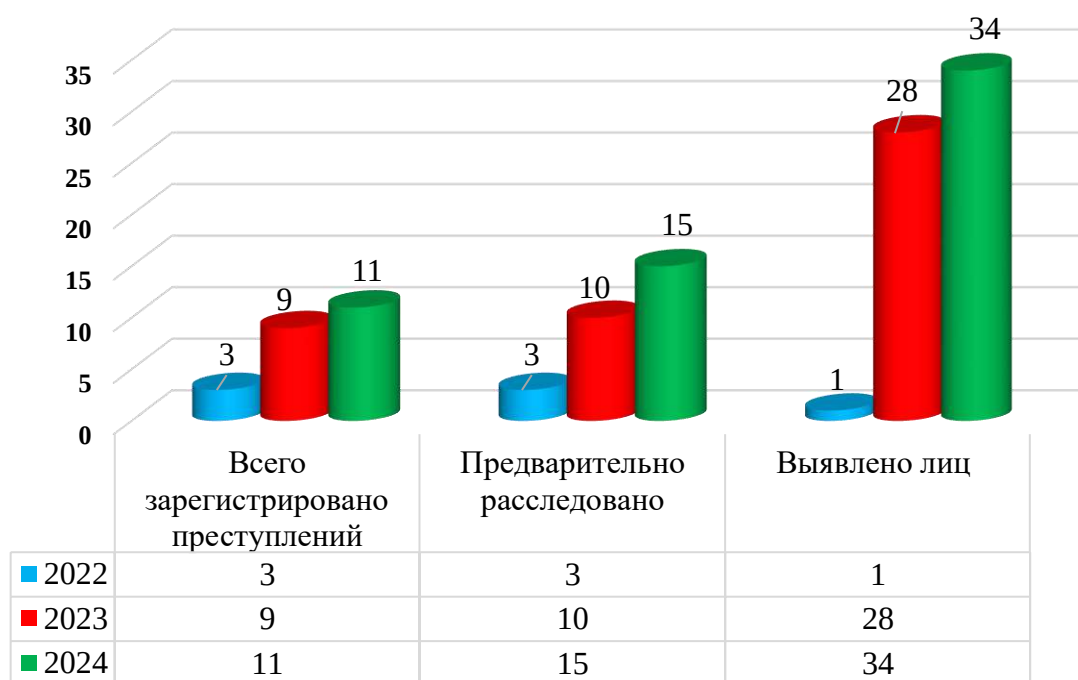


Диаграмма 8. Уголовные дела, возбужденные по ст. 210 УК РФ
(включая экономические составы)

По прежнему самым распространённым видом преступления является мошенничество, совершенное от имени государственных служащих, сотрудников банков под предлогом перевода денежных средств на «безопасный» счет. Вместе с тем организаторы мошеннических колл-

центров адаптируются под современные реалии и используют их для обмана граждан, как бы подтверждая криминальную версию. Так, в связи с проведенными в 2023 году Минцифры России мероприятиями по проверке абонентских номеров через портал «Госуслуги», предусмотренными Федеральным законом от 30 декабря 2020 г. № 533-ФЗ «О внесении изменений в Федеральный закон «О связи»³⁵, мошенники стали осуществлять звонки от имени сотрудников оператора связи и сообщать, что необходимо продлить договор оказания услуг либо подтвердить личность, просить продиктовать код из СМС, который является одноразовым кодом доступа к личному кабинету гражданина на портал. После получения доступа на портал мошенничество развивается сразу по двум сценариям. Преступники получают возможность подать заявки на кредиты, а также займы от имени потерпевшего, похитив электронные образцы документов, а также звонить от имени сотрудников государственных учреждений и силовых ведомств с требованием перевода денежных средств на безопасный счет.

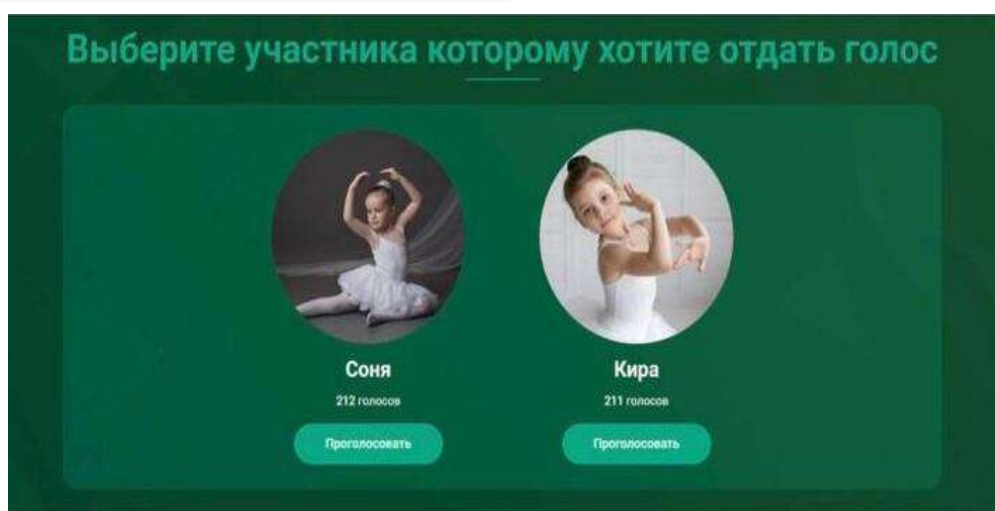
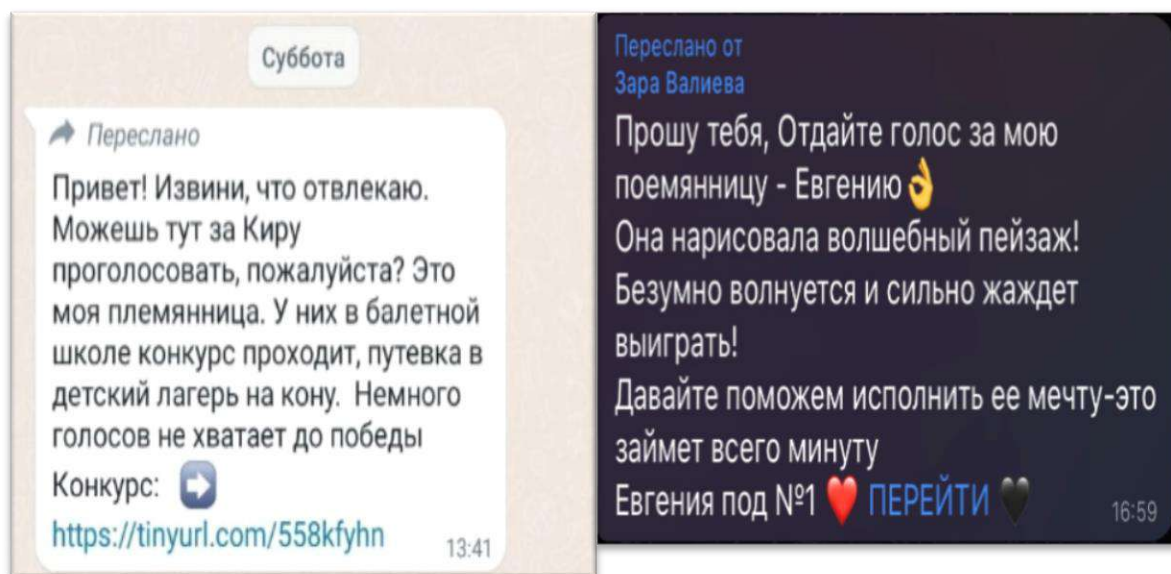
По сведениям подсистемы «Дистанционное мошенничество» программно-технического комплекса интегрированного банка данных федерального уровня (далее – ПТК «ИБД-Ф») за 2023 год по преступлениям, совершенным путем звонков от имени оператора связи, возбуждено 584 уголовных дела.

Кроме того, в связи с возрастанием роли в нашей жизни онлайн-порталов (Госуслуги, Mos.ru), позволяющих дистанционно предоставлять услуги, возросло количество преступлений, совершаемых под предлогом их взлома. Несмотря на новый предлог, в конечном итоге указанная схема мошенничества заканчивается переводом денежных средств на «безопасный счет». По сведениям подсистемы «Дистанционное мошенничество» ПТК «ИБД-Ф» за 2023 год по преступлениям, совершенным указанным способом, возбуждено 450 уголовных дел.

В 2023 году начались массовые атаки на российских пользователей популярных мессенджеров WhatsApp и Telegram. Злоумышленники с применением технологий социальной инженерии получали возможность изучения аккаунта и управления им. В ходе проведенных мероприятий совместно с АО «Лаборатория Касперского» установлена вся схема преступления. Исходя из схемы, жертва получает сообщение от абонента из списка своих контактов с просьбой проголосовать за племянницу (знакомую, подругу и т. д.), которая участвует в конкурсе. Сообщение содержит ссылку публичного сервиса коротких ссылок. При переходе

³⁵ О внесении изменений в Федеральный закон «О связи»: Федеральный закон от 30 декабря 2020 г. № 533-ФЗ // Информационно-правовой портал «Гарант.Ру». – URL: <https://www.garant.ru/products/ipo/prime/doc/400058624/> (дата обращения: 25.12.2025).

по ссылке осуществляется перенаправление на сайт *Evernote* <https://evernote.com/intl/ru> (веб-сервис и набор программного обеспечения для создания и хранения заметок). При переходе по гиперссылке [перейти к голосованию] осуществляется перенаправление на фишинговую страницу, где необходимо «Авторизоваться, чтобы проголосовать» (рис. 41).



Чтобы отдать свой голос, перейдите по ссылке, указанной ниже и следуйте инструкции:

➡ **ПЕРЕЙТИ К ГОЛОСОВАНИЮ** ⬅

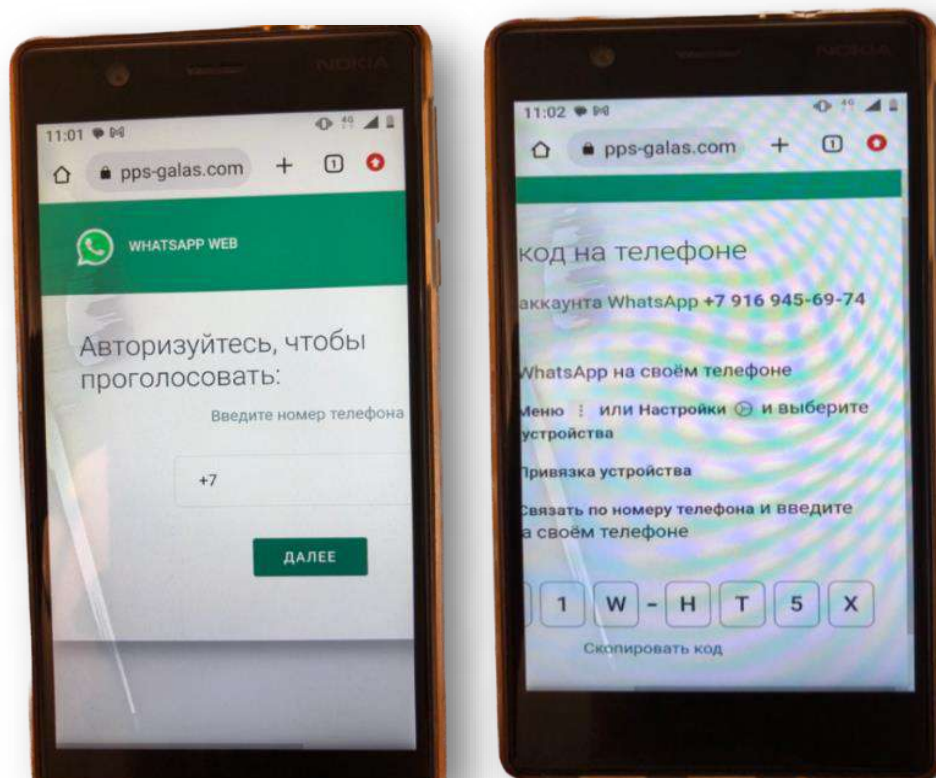


Рис. 41. Схема дистанционного хищения посредством использования сервисов для обмена сообщениями через Интернет

В действительности указанная страница транслирует форму добавления к учётной записи мессенджера WhatsApp связанного (дополнительного) устройства. Таким образом злоумышленники получают доступ к аккаунту жертвы. Фишинговая страница голосования располагается на временных доменах вида: betup88-mahaheng.com или blcapitalinvest.com/5ucs/. Часть доменов соответствуют серверу **193.107.109.81** (украинский хостер «Хостико»). Оба сервера географически расположены в Германии. В результате проверки на ресурсе *VirusTotal* установлено, что на сервер 193.107.109.81 в разное время ссылалось более 200 доменов.

После получения доступа преступники некоторое время изучают личность потерпевшего и в зависимости от полученной информации развивают преступление по двум схемам:

- определив, в какой организации работает потерпевший, злоумышленники создают подложные учетные записи от имени должностных лиц, занимающих руководящие должности. Затем размещают в профилях их фотографии, скаченные из открытых источников в сети Интернет, после чего направляют сообщения должностным лицам, находящимся в подчинении у лиц, чьими именами представляются, с указанием ожидать звонка

от сотрудников ФСБ России для дальнейших действий. Затем со скрытого аккаунта поступает звонок от неустановленного лица, которое, представляясь сотрудником ФСБ России, сообщает о списаниях с банковского счета средств в поддержку террористических организаций и под предлогом обеспечения безопасности денежных средств убеждает осуществить перевод денег на «безопасный счет»;

- со взломанного аккаунта коллеги/знакомому потерпевшему приходит сообщение с просьбой занять денег, дополнительно мошенники присылают фотографию карты, куда нужно перевести деньги.

После изучения финансовой стороны данного вида преступлений было установлено, что лица, совершая мошеннические действия для вывода денежных средств, добытых криминальным путем, массово использовали банковские карты ООО «Озон Банк».

В ходе устранения благоприятных условий, способствующих совершению преступлений, с целью профилактического воздействия сотрудниками оперативных подразделений ФСБ России и МВД России совместно с Минцифры России на территории Российской Федерации был заблокирован весь пул IP-адресов, выделенный украинской компании «Хостико». Также в ходе совместной рабочей встречи руководство ООО «Озон Банк» проинформировано о совершаемых преступлениях с использованием карт указанной организации, в результате чего приняты меры, направленные на блокировку подозрительных транзакций и карт, выявленных антифрод-системой. Результатом стало снижение регистрации указанных преступлений.

Вместе с тем по итогам 2023 года к самым распространённым видам и способам преступлений, совершенных дистанционным способом, можно отнести звонки:

- от имени государственных служащих, сотрудников банков под предлогом перевода денежных средств на безопасный счет – 21 523;

- в отношении клиентов торговых интернет-площадок под предлогом покупки/продажи товара либо совместной поездки на автомашине через сервис автопутешествий – 13 653;

- под предлогом займа денег и посредством скомпрометированной учетной записи – 6 548;

- под предлогом освобождения от уголовной ответственности («сын попал в беду») – 1 762.



Диаграмма 9. Наиболее распространённые виды и способы преступлений, совершенные в современном информационном пространстве с использованием сети Интернет дистанционным способом

В связи с принятыми изменениями в Федеральный закон «О связи» от 7 июля 2003 г. № 126-ФЗ³⁶ и внесениями поправок в КоАП РФ, ГУ организована работа по привлечению к административной

³⁶ О связи: Федеральный закон от 7 июля 2003 г. № 126-ФЗ // СПС «КонсультантПлюс»: [сайт]. – URL: https://www.consultant.ru/document/cons_doc_LAW_43224/ (дата обращения: 25.12.2025).

ответственности юридических лиц, осуществляющих пропуск подменных номеров на территорию Российской Федерации.

В результате совместных усилий государственных органов по привлечению операторов связи к административной ответственности по ст. 12.2.1 КоАП РФ преступники потеряли возможность осуществлять звонки с подмененных официальных абонентских номеров госорганов.

Несмотря на принятые меры, в ходе анализа оперативной обстановки выявлены распространённые способы осуществления мошеннических звонков:

➤ Удаленный доступ к абонентскому номеру с использованием официального приложения (мессенджера), предоставленного оператором связи (ПАО «Мегафон» – Emotion, ПАО «МТС» – Мой Коннект).

Техническими особенностями указанных мессенджеров является возможность осуществления звонков с абонентского номера иного устройства, т. е. без сим-карты, в случае подтверждения входа в приложения через смс, поступившее на абонентский номер. В результате указанных технических возможностей соучастники мошенников-операторов колл-центров, находясь на территории Российской Федерации, активируют для них удаленный доступ к мессенджерам.

➤ Аренда виртуальной АТС.

Данная услуга распространена в ПАО «Вымпелком». Преступники арендуют несколько абонентских номеров, которые работают как «карусель», в результате чего оператор связи не имеет возможности идентифицировать абонентский номер, с которого в настоящий момент осуществляется звонок. Данную услугу предоставляет не ПАО «Вымпелком», а оператор, который по договору оферты получил номера как клиент. Одним из таких операторов является ООО «Зорро». В настоящее время УУР ГУ МВД России по г. Москве изучает возможность привлечения к ответственности ООО «Зорро» и иные организации, передающие клиентам в пользование абонентские номера, выделенные иным операторам связи.

➤ Дистанционная аренда абонентских номеров у операторов, предоставляющих услуги IP-телефонии через проданные либо похищенные аккаунты портала Госуслуг.

В настоящее время участники международных организованных преступных сообществ, находящиеся за пределами территории РФ, с целью осуществления противоправной деятельности привлекают соучастников, которые осуществляют подбор студентов, лиц, ведущих антиобщественный образ жизни, и регистрируют их как индивидуальных предпринимателей, после чего, получая доступ к странице Госуслуг, передают его мошенникам, которые подтверждают через нее аренду абонентских номеров, в том числе

с географически определяемым планом нумерации (8 800 ***-**-**, 8 495 ***-**-**, 8 499 ***-**-** и др.).

➤ Получение удаленного доступа к мессенджеру.

Самым распространённым способом звонков мошенниками из-за рубежа является получение удаленного доступа к мессенджерам через сайт СМС-активатор, который, в свою очередь, осуществляет свою деятельность с помощью SIM-боксов и SIM-банков. В результате проведенных в 2023 году мероприятий проведено 9 обысков на территории различных регионов страны и изъято более 100 SIM-боксов и более 3 000 SIM-карт различных операторов связи.

В 2023 году стали трансформироваться и преступные схемы вывода денежных средств, добытых преступным путем, в наличный оборот.

Так, все чаще участники организованных преступных групп (далее – ОПГ) и организованных преступных сообществ (далее – ОПС) не снимают денежные средства с карт третьих лиц, а, получив их от потерпевших, совершают обмен на популярных криптовалютных площадках. Денежные средства получает неосведомленный гражданин, осуществляющий спекуляцию на курсе криптовалюты. В данном случае особое значение имеет изучение выписок первой карты, на которую переведены денежные средства потерпевшего. Особенно необходимо обратить внимание на информацию об IP-адресах входа в онлайн-банк, а также абонентских номерах, привязанных к картам. Кроме того, в большинстве случаев преступники в ходе введения в заблуждение потерпевшего просят его установить на свой смартфон приложение «Мир Пэй» и привязать банковские карты, открытые на так называемых «дропов», объясняя это тем, что указанные карты/счета являются «безопасными». После этого денежные средства обналичиваются в банкоматах соучастниками, либо по вышеуказанной схеме осуществляется обмен на криптовалюту. Принятыми мерами удалось устранить возможность использования в преступных целях карт и кошельков ЗАО «Киви Банк» и ООО «Озон Банк». Вместе с тем некоторые банковские организации самостоятельно устранили возможность пополнения своих карт денежными средствами потерпевших, которые подключили их к своим устройствам через приложение «Мир Пэй», введя так называемый «период охлаждения». Новшество заключается во введении временного интервала в 48 часов между подключением карты в приложении и возможностью пополнять ее наличными денежными средствами. Такой положительный опыт позволил значительно снизить возможность использования преступниками карт Банка «ВТБ» (ПАО). Несмотря на это, лица, вынашивающие преступный умысел, сориентировались и в настоящее время используют для

вывода денежных средств банковские карты ПАО «Росбанк», АО «Райффайзенбанк».

В 2023 году в суды города Москвы направлено два уголовных дела, возбужденных по ч. 1, ч. 2 ст. 210 УК РФ в отношении соучастников украинских колл-центров, осуществляющих обналичивание денежных средств.

Приведем и рассмотрим пример ОПС И. М. Згнетова:

Сотрудниками УУР задокументирована деятельность преступного сообщества, участники которого в период с февраля 2020 г. по 19 августа 2021 г., находясь на территории Российской Федерации и Украины, совершали хищения денежных средств дистанционным способом у пожилых жителей г. Москвы и других регионов России посредством звонков от имени сотрудников ПАО «Сбербанк» и правоохранительных органов под предлогом обеспечения сохранности и целостности вкладов, убеждали их переводить денежные средства на предоставленные «безопасные» счета.

Установлено, что участники преступной организации обоснованно причастны к совершению преступления в отношении внучки легендарного летчика – О. В. Чкаловой. По данному факту 13.04.2021 возбуждено уголовное дело № 12101450137000240 по признакам преступления, предусмотренного ч. 4 ст. 159 УК РФ, находящееся в производстве 9 отдела СЧ ГСУ ГУ МВД России по г. Москве.

В августе 2021 г. в ходе реализации оперативной информации сотрудниками УУР ГУ МВД России по г. Москве на территории Омской области, Республики Бурятия и Хабаровского края задержаны 10 лиц, причастных к совершению указанного преступления и действующих под руководством И. М. Згнетова. 10 июня 2022 г. принято решение о выделении и возбуждении в отношении них уголовного дела № 12201450179002245 по ч. 1, 2 ст. 210 УК РФ.

Приведем и рассмотрим пример ОПС А. Г. Балояна:

В рамках расследования уголовного дела № 12001450006000547, возбужденного 30.07.2020 СУ УВД по ЮЗАО ГУ МВД России по г. Москве по признакам преступления, предусмотренного п. «б» ч. 4 ст. 158 УК РФ, находящегося на оперативном сопровождении сотрудников ОУР УВД по ЮЗАО ГУ МВД России по г. Москве. Предпринятыми мерами удалось установить причастность к совершению вышеуказанного преступления 14 фигурантов под руководством А. Г. Балояна. В отношении участников выделено уголовное дело по ч. 1 и 2 ст. 210 УК РФ. В июне 2023 г. уголовное дело направлено в Таганский районный суд, где в зале судебного заседания в соответствии с действующим уголовно-процессуальным законодательством был вынесен обвинительный приговор.

В тесном взаимодействии УУР и УБК ГУ МВД России по г. Москве постоянно проводится следующая управленческая и профилактическая работа:

1. С учетом активизации совершения дистанционных мошенничеств в отношении граждан пожилого возраста, сопряженных с продажей недвижимого имущества, для риэлторов разработан алгоритм действий, необходимый для пресечения совершения данного вида преступлений, а также информирования сотрудников полиции о фактах их совершения. Данный алгоритм и памятка для граждан размещены в риэлтерских агентствах г. Москвы.

В ходе взаимодействия с риэлторскими агентствами и ОУР УВД по АО ГУ МВД России по г. Москве удалось предотвратить хищение 68 квартир.

2. В целях своевременного информирования граждан о появлении новых видов дистанционных хищений заключено соглашение с правительством Москвы о проведении профилактических мероприятий. При непосредственном консультативном участии сотрудников УУР ГУ МВД России по г. Москве администрируется сайт «Перезвони Сам».

3. Организовано взаимодействие с Департаментом информационных технологий г. Москвы по вопросу профилактики хищений денежных средств, совершенных дистанционным способом, в том числе у лиц пожилого возраста и иных социально незащищенных категорий населения в сфере завладения недвижимым имуществом граждан, а также дистанционных хищений на электронных торговых площадках. Соответствующие профилактические материалы, в том числе памятки, направлены в Департамент информационных технологий г. Москвы для размещения на интернет-ресурсах различных организаций.

4. С участием Департамента информационных технологий г. Москвы подготовлены и проведены три профилактических вебинара.

5. В Банк России подготовлено информационное письмо о сервисах АО «Альфа-банк», создающих условия для совершения дистанционных хищений: возможность осуществления переводов денежных средств через банкоматы по номеру счета, без физического использования банковской карты, а также увеличение лимита на снятие денежных средств с одной карты до 3 млн руб. в день. В результате зафиксировано снижение использования в преступных целях продуктов указанного банка.

6. В связи с тем, что платежная система Qiwi чаще всего используется для вывода денежных средств, добытых преступным путем, за пределы страны, по совместной инициативе ГУ МВД России по г. Москве и ФСБ России 9 февраля 2023 г. электронная платежная система Qiwi внесена в реестр организаторов распространения информации, что обязывает ее хранить

сведения обо всех действиях и взаимодействиях пользователей, по первому требованию предоставлять их правоохранительным органам. В результате зафиксировано снижение использования в преступных целях продуктов указанного банка.

7. В рамках деятельности рабочей группы, созданной на базе Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации при участии ГУ МВД России по г. Москве с целью противодействия правонарушениям и преступлениям, совершаемым в современном информационном пространстве с использованием сети Интернет, проводится профилактическая работа по выявлению и блокировке деятельности на территории Российской Федерации операторов связи, действующих в нарушение законодательства. В результате проведенной работы заблокировано более 60 организаций.

8. Регулярно проводятся рабочие совещания с сотрудниками и руководителями 4 отделений ОУР УВД по АО с приглашением специалистов банковского сектора и IT-сферы на темы:

- технология борьбы с киберпреступлениями, предотвращение кибератак, выявление мошенничеств, совершенных дистанционным способом;
- криминалистика блокчейнов, отслеживание биткоинов и других криптовалют в ходе расследования;
- виды электронных следов преступника, хранящиеся в базах данных ПАО «Сбербанк России», способы их получения;
- повышение эффективности деятельности по противодействию дистанционным хищениям общеуголовной направленности, в том числе новым формам и способам совершения данных преступлений.

9. Проведено совещание с представителями компаний каршеринга ООО «Каршеринг Россия» (Делимобиль), АО «Каршеринг» (BelkaCar), ООО «Яндекс Драйв» по вопросу принятия дополнительных мер к пресечению использования водителями автомобилей-каршерингов подложных аккаунтов, а также установлению и привлечению к ответственности лиц, распространяющих предложения об их покупке. По результатам принято решение о проработке вопроса заключения соглашения об электронном взаимодействии с ГУ МВД России по г. Москве, в том числе с целью проверки сотрудниками ГУ МВД России по г. Москве действительности водительских удостоверений.

10. Направлена законодательная инициатива о необходимости внесения изменений в ФЗ «О связи», закрепляющих возможность оформления договоров об оказании услуг связи операторами иностранным гражданам и лицам без гражданства исключительно в офисах операторов связи при предъявлении документа, удостоверяющего личность, а также исключение возможности делегирования полномочий оформления договоров об оказании

услуг связи с физическими и юридическими лицами «уполномоченным лицам», не имеющим лицензии на деятельность в области оказания услуг связи, предусмотрев введение ответственности операторов за несоблюдение указанных норм.

11. Систематически при руководстве УУР и УБК ГУ МВД России по г. Москве проходят совещания с представителями кикшеринговых компаний ООО «ВУШ», ООО «КИК», ООО «Шеринговые технологии» (аренда электросамокатов и велосипедов), на которых принимаются решения о проработке вопросов заключения соглашения об электронном взаимодействии с ГУ МВД России по г. Москве.

12. Систематически при руководстве УУР и УБК ГУ МВД России по г. Москве проходят совещания с руководителем службы безопасности ПАО «Уралсиб», на которых принимаются решения о проработке вопросов оперативного взаимодействия и возможности заключения соглашения об электронном взаимодействии с ГУ МВД России по г. Москве.

13. При непосредственной консультации ГУ МВД России по г. Москве на каналах центрального телевидения России регулярно транслируются репортажи о мерах, предпринимаемых полицией по борьбе с мошенниками, и мерах, которые необходимо предпринимать, чтобы не стать их жертвой.

14. С привлечением блогеров, таких как Спартак Бендеров (более 2 000 000 подписчиков), на каналах различных информационных платформ публикуются видеоролики для лиц от 14 до 20 лет, в которых содержится информация о возможных последствиях передачи банковской карты, открытой на свое имя, третьим лицам.

15. ФСБ России совместно со специалистами ООО «Инфомедиа» постоянно разрабатываются профилактические ролики, содержащие информацию о популярных предложениях, используемых мошенниками.

Выявление, пресечение и раскрытие преступлений в сфере противоправного использования информационно-коммуникационных технологий является одним из приоритетных направлений оперативно-служебной деятельности органов внутренних дел.

В соответствии с приказом Главка от 7 июня 2022 г. № 199 «Об определении полномочий оперативных подразделений системы ГУ МВД России по г. Москве по противодействию преступлениям, совершенным с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации», 32 состава преступлений, совершенных с использованием ИКТ или в сфере компьютерной информации, отнесены к компетенции Управления по борьбе с противоправным использованием информационно-коммуникационных технологий.

По итогам 6 месяцев 2025 г. на территории г. Москвы зарегистрировано 31 032 (–769; –2,4 %) преступления, совершенного с использованием ИКТ или в сфере компьютерной информации, их доля в общем массиве преступлений составила 47,1 % (всего в г. Москве зарегистрировано 65 875 преступлений).

Из общего количества зарегистрированных преступлений, совершенных с использованием ИКТ: экономической направленности – 4 376 (2024 – 4 012, +9,1 %); общеуголовной направленности – 26 656 (2024 – 27 789, –4,1 %), из них связанных с НОН – 4 887 (2024 – 2 969, –64,6 %), экстремистской направленности – 59 (2024 – 45, +31,1 %), террористического характера – 44 (2024 – 51, –13,7 %). Дистанционные хищения составляют 75 % ИКТ-преступлений.

В отчетном периоде сотрудниками УБК ГУ МВД России по г. Москве задержано 32 лица. Пресечена противоправная деятельность 6 организованных групп. На оперативном сопровождении УБК ГУ состоят 33 уголовных дела по более чем 400 эпизодам преступной деятельности (предварительно в ОГ – более 300). В ходе работы осуществлено 14 выездов в служебные командировки по сопровождаемым уголовным делам (*перспектива реализации во II полугодии – по 11 уголовным делам*). Возбуждено 2 уголовных дела по ч. 1, 2 ст. 210 УК РФ.

Согласно сведениям Зонального информационного центра ГУ МВД России по г. Москве (ЗИЦ), во II квартале 2025 г. статистические показатели Управления в сравнении с аналогичным периодом прошлого годакратно увеличились.

Так, сотрудниками УБК ГУ в 2025 году раскрыто на 141 преступление больше, чем в 2024 (152; 2024 – 11), из них ТиОТ³⁷ – 116, ППЛ – 52, ОГиПС – 34. Выявлено 156 преступлений, что на 116 больше (2024 – 40), из них ТиОТ – 112, ОГиПС – 6. Показатель направленных в суд уголовных дел увеличился более чем в два с половиной раза (58; +37; 2024 – 21), из них ТиОТ – 23, ОГиПС – 5, ППЛ – 1.

Преступления, относящиеся к компетенции Управления по борьбе с противоправным использованием информационно-коммуникационных технологий ГУ МВД России по г. Москве, по большей части отличаются значительной общественной опасностью и зачастую вызывают широкий общественный резонанс.

Например, по результатам проведения комплекса оперативно-розыскных мероприятий по проверке информации из базы данных Генерального секретариата Интерпола, содержащей изображения несовершеннолетних, подвергшихся сексуальному насилию (International Child Sexual Exploitation Database, ICSE DB), сотрудниками УБК ГУ МВД России по г. Москве

³⁷ ТиОТ – тяжкие и о особо тяжкие преступления.

во взаимодействии с УБК МВД России и ДВКР ФСБ России задержан и заключен под стражу Козлов Денис Валерьевич, 6 января 1988 года рождения, старший научный сотрудник 55-го отдела 3-го ЦНИИ Министерства обороны Российской Федерации, который с 2022 года совершал насильственные действия в отношении своей дочери, не достигшей 14-летнего возраста, не осознающей характер и значение совершаемых действий, то есть находящейся в беспомощном состоянии, склонял к систематическому фотографированию с демонстрацией половых органов. Фото- и видеоизображения распространялись Д. В. Козловым в тематических сообществах иностранного сегмента сети Интернет. По результатам осмотра изъятого технического устройства установлена причастность более чем к 160 эпизодам преступной деятельности, предусмотренной ч. 4 ст. 132 УК РФ.

Расследование организовано военным следственным отделом Следственного комитета Российской Федерации по Одинцовскому гарнизону в рамках уголовного дела № 12502003308000373, возбужденного по признакам преступления, предусмотренного п. «б» ч. 4 ст. 132, п. «в» и «г» ч. 2 ст. 242.2 Уголовного кодекса Российской Федерации.

Помимо того, лица, совершающие ИКТ-преступления, при формировании предлогов и способов противоправной деятельности активно используют современные технологические решения.

Так, сотрудниками УБК ГУ МВД России по г. Москве задокументирована и пресечена деятельность преступной группы в составе Д. Ю. Титова и Э.И. Мурсалова, которые путем адресной мошеннической атаки в отношении руководителя крупной московской IT-компании (владельца дата-центров) в онлайн-игре World of Warcraft, а также с использованием мессенджера Discrod, в период времени с 2023 по 2024 год, представляясь сотрудниками ЦРУ, под угрозой блокирования деятельности компании, осуществили хищение денежных средств свыше 154 млн руб.

Результаты оперативно-розыскной деятельности рассекречены и представлены в СО ОМВД России по району Соколиная гора г. Москвы для приобщения к материалам уголовного дела № 12501450053000085, расследуемого по признакам преступления, предусмотренного ч. 4 ст. 159 УК РФ, с квалифицирующим признаком «совершено в особо крупном размере».

Следует отдельно отметить, что сотрудниками УБК произведена первая в России реализация оперативной информации по преступлению, предусмотренному ч. 3 ст. 187 Уголовного кодекса, предусматривающей ответственность за передачу третьим лицам из корыстной заинтересованности электронных средств платежа и осуществление неправомерных операций³⁸.

22 июля 2025 г. УБК ГУ в рамках УД 382 задержана Коломиченко Евгения Анатольевна, 1973 года рождения, которая из корыстной

³⁸ О внесении изменений в статью 187 Уголовного кодекса: Федеральный закон от 24 июня 2025 г. № 176-ФЗ // СПС «КонсультантПлюс»: [сайт]. – URL: https://www.consultant.ru/document/cons_doc_LAW_508353/ (дата обращения: 21.12.2025).

заинтересованности по указанию неустановленных лиц в мессенджере Telegram оформила на свое имя юридическое лицо, с использованием которого выпустила 37 банковских карт. Указанные платежные инструменты передала в пользование заказчикам.

В целях совершенствования организации борьбы с ИКТ-преступлениями, *приказом ГУ МВД России по г. Москве от 7 мая 2025 г. № 146* утверждено Положение о координации деятельности подразделений системы ГУ МВД России по г. Москве по борьбе с преступлениями, совершаемыми с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации.

В отчетном периоде проведена работа по профилактике ИКТ-преступлений, в том числе *распоряжением ГУ МВД России по г. Москве от 28 мая 2025 г. № 1/8113* утвержден Алгоритм профилактических мероприятий по дистанционным хищениям, регламентирующий порядок действий по данному направлению для всех подразделений Главка.

В отчетном периоде руководство Управления неоднократно принимало участие в тематических сюжетах в СМИ, круглых столах, вебинарах, освещающих наиболее распространенные способы (виды) совершения хищений денежных средств дистанционным способом и методы противодействия, а также механизмы вовлечения граждан в преступную деятельность и последствия продажи электронных средств платежа или передачи права их использования третьим лицам.

Для повышения уровня квалификации сотрудников специализированных подразделений Главка УБК проведены обучающие занятия по выявлению, документированию и раскрытию ИКТ-преступлений, в которых приняли участие свыше 300 сотрудников подразделений окружного и районного уровней. Разработаны и направлены в подразделения алгоритмы и методические рекомендации.

В 2025 году на территории г. Москвы сотрудниками УБК ГУ МВД России по г. Москве проведено 5 оперативно-профилактических мероприятий по линии ИКТ и компьютерной информации, направленных на документирование и пресечение преступной деятельности лиц, распространяющих материалы порнографического характера с участием несовершеннолетних; преступлений, связанных с незаконным оборотом персональных и иных охраняемых законом данных; противоправной деятельности участников колл-центров, использующих SIM-банки и SIM-боксы; выявление фактов незаконной реализации SIM-карт.

По результатам возбуждено 29 уголовных дел по указанным направлениям противоправной деятельности, задержано и привлечено к ответственности 59 лиц, проведено 437 проверок в порядке ст. 144–145 УПК РФ, заблокировано 608 информационных ресурсов с противоправным контентом, пресечено функционирование 3 крупных

локализаций криминального телефонного трафика. Изъято 130 SIM-боксов, 59 преобразователей волновых полей и 4 сетевых коммутатора («Switch HUB»).

Вместе с тем в ходе организации работы по выявлению, пресечению и раскрытию ИКТ-преступлений сотрудниками различных подразделений Главка выявлен ряд проблемных вопросов.

Так, в нарушение разработанных алгоритмов в ряде случаев при поступлении заявления о дистанционном хищении сотрудниками территориальных подразделений не должным образом проводятся мероприятия по установлению курьеров, в частности отработка камер видеонаблюдения ЕЦХД³⁹ и частных (коммерческих), проведение мероприятий по установлению и задержанию транспортных средств по горячим следам.

Срок хранения видеозаписей ЕЦХД составляет 5 дней, фотографии – до 30 дней. Срок хранения коммерческих записей не ограничен.

Пример: в сводку от 6 июля помещены сведения о раскрытом дистанционном мошенничестве в ОМВД по району Северное Измайлово (УД № 12501450052000355 по ч. 4 ст. 159 УК РФ). Задержана женщина 1945 года рождения. Установлено, что указанная женщина является курьером первого звена. В течение двух суток с подачи заявления видео не изъято, автомобили курьеров не задержаны, местонахождение похищенных денежных средств не установлено.

После установления контроля за работой по преступлению выяснилось, что в местах передачи потерпевшей денежных средств есть частные камеры видеонаблюдения, и записи на них сохранены. В результате по цепочке задержаны еще три подозреваемых, причастных к совершению преступления. Всем предъявлены обвинения. Деньги перечислены через криптобиржу в Москве-Сити. Вместе с тем при своевременной и надлежащей организации работы «по горячим следам» перевод денежных средств мог быть предотвращен.

Ненадлежащим образом организована работа по контролю за соблюдением приказа ГУ МВД России по г. Москве от 5 апреля 2021 г. № 121 «О порядке формирования, ведения и использования подсистемы «Дистанционное мошенничество» ПТК «ИБД-Ф» в ГУ МВД России по г. Москве». По-прежнему наблюдаются факты невнесения сведений в подсистему, несвоевременного внесения либо неинформативного их внесения.

Пример: Южное Медведково, УД № 254 (ст. 159 УК РФ, от 10 июля 2025 г.). Фабула: «Звонок от правоохранительных органов под предлогом

³⁹ Единый центр хранения и обработки данных (ЕЦХД) – это государственная цифровая система г. Москвы для сбора данных с камер видеонаблюдения, установленных в общественных местах. Основная цель этой платформы – обеспечение безопасности жителей столицы. Оперативное управление системой осуществляет Департамент информационных технологий г. Москвы.

участия в ОРМ убедили потерпевшую положить денежные средства в почтовый ящик в подъезде». В карточке ПТК «ИБД-Ф» указано: «Звонили неизвестные, под предлогом сохранения денежных средств от мошенников убедили передать деньги через почтовый ящик тремя платежами».

Следующая проблема – по большинству суточных сводок по дистанционным хищениям, поступающим в Главк, отсутствуют предлог и способ совершения преступления. Ограничиваются фразами: «сохранение денежных средств», «резервный счет».

Пример: Люблино, УД № 738 (ст. 159 УК РФ, от 14 июля 2025 г.). В карточке ПТК «ИБД-Ф» указано дословно: «неустановленные лица похитили денежные средства, принадлежащие В. И. Бакотину, на сумму 552 000 руб., а также денежные средства на сумму 1 104 000 руб., принадлежащие Т. И. Сазоновой». То есть в фабуле нет способа, предлога, информации о курьерах.

В ходе проверок по дистанционным хищениям, при совершении которых деньги потерпевшими переводятся через приложение NFC-Gate, а также с использованием вредоносных APK-файлов, не производится их качественный осмотр. В случаях, когда мобильный телефон изымается, в большинстве случаев осмотры производятся оперативными службами, несмотря на наличие в ЭКЦ УВД по АО экспертов.

Пример: Царицыно, УД № 388 (ст. 158 УК РФ, от 15 июля 2025 г.). При совершении дистанционного хищения неустановленные лица убедили потерпевшую установить на мобильный телефон неизвестное приложение и поднести карту к телефону, в результате чего начали происходить списания денежных средств. То есть в ходе опроса уже очевидно, что произведена токенизация карты с использованием приложения типа NFC-Gate. Однако, телефон при обращении заявителя не осматривался и не изымался.

Вместе с тем 27 июня 2025 г. издано и направлено для исполнения распоряжение Министра внутренних дел № 1/8169, в соответствии с которым необходимо изымать у заявителя средства мобильной связи с признаками наличия вредоносного программного обеспечения (ВПО) и направлять для проведения осмотра в подразделение по борьбе с киберпреступностью, а также организовать обучение сотрудников оперативных подразделений и органов предварительного расследования навыкам проведения осмотров средств мобильной связи на предмет выявления вредоносных APK-файлов.

Проблемные вопросы возникают также и при осуществлении профилактической деятельности. Ненадлежащим образом организована работа по привлечению операторов связи к административной ответственности по фактам нарушения положений ст. 13.2.1 и 13.29 КоАП РФ, а также требований ст. 44 ФЗ «О связи».

В первом полугодии вынесено всего 20 судебных решений в отношении организаций и лиц, допустивших пропуск в сеть трафик «подменного номера», и подготовлено более 50 материалов об использовании «обезличенных» сим-карт либо оформленных на подставных лиц, при том, что с мая по июль 2025 года зарегистрировано 88 дистанционных хищений, совершенных с использованием абонентских номеров с префиксами 495, 499, и 2 333 таких преступления, совершенного с использованием мобильных абонентских номеров.

Не менее важной и актуальной проблемой является недостаточное материально-техническое оснащение специализированных подразделений по ИКТ-преступлениям.

В ходе проверки и оказания практической и методической помощи УВД по АО и ОМВД России по районам г. Москвы выявлено отсутствие в ряде подразделений компьютеров, подключенных к сети Интернет, специального программного обеспечения и аппаратно-программных комплексов (для мониторинга сети Интернет, выявления противоправного контента, проведения ОРМ и анализа больших данных), проекторов и интерактивных досок (для обучения личного состава и презентаций по профилактике).

Пример: в ОУР УВД по ВАО, СВАО, ЮАО, ОМВД России по Бабушкинскому и Ярославскому районам, а также по районам Богородское и Северное Измайлово г. Москвы отсутствует подключение к сети Интернет.

В настоящее время для совершенствования организации работы по направлениям деятельности УБК совместно с Главным следственным управлением и прокуратурой г. Москвы прорабатывается вопрос о выработке единой позиции по порядку возбуждения уголовных дел по преступлениям, связанным с неправомерным доступом к компьютерной информации.

Помимо того, запланировано провести дополнительное обучение по противодействию данному виду преступлений сотрудников территориальных отделов МВД России по районам г. Москвы.

УБК ГУ МВД России по г. Москве на постоянной основе проводится анализ эффективности оперативно-служебной деятельности. На протяжении нескольких лет динамика результативности повышается. Вместе с тем оперативная обстановка по линии ИКТ остается сложной в связи с большой регистрацией и периодическим появлением новых способов совершения преступлений.

Заключение

Свобода и желание каждого участника информационного пространства проявить себя как индивидуальная личность позволяет преступным элементам действовать дерзко и безбоязненно, в связи с чем возможно утверждать, что информатизация общества, обладая, несомненно, множеством положительных сторон, привела и к информатизации криминальной среды, придала ей ярко выраженный интернациональный и высокотехнологичный характер. Лица, склонные к совершению вышеуказанных преступлений, используют возможности IT-технологий, что способствует расширению транснационального масштаба, и, как результат, в конечном итоге определяют и создают угрозу национальной безопасности.

На протяжении многих лет сотрудники органов внутренних дел ведут упорную борьбу, направленную на своевременное предупреждение, выявление, раскрытие и успешное расследование преступлений, совершаемых с использованием возможностей IT-технологий. Способы совершения преступлений постоянно видоизменяются, в механизм совершения преступлений вносятся новые изощренные схемы, в связи с чем раскрытие указанных преступлений становится затруднительным. Такое положение требует от сотрудников правоохранительных органов своевременного получения специальных знаний, умений и навыков в указанной сфере.

Для решения данной задачи необходимо постоянно вести активную работу по подготовке учебно-методических материалов с освещением практического опыта раскрытия рассматриваемых видов преступлений, что благоприятно будет сказываться на профессиональных компетенциях сотрудников органов внутренних дел.

Очевидно, преступления, совершаемые с использованием IT-технологий, носят корыстный характер. Все чаще мы сталкиваемся с таким распространенным видом преступлений, как мошенничество, которое в настоящее время практически каждый день совершается разными изощренными способами.

Преступления, совершаемые в этой сфере, позволяют преступникам анонимизироваться. Высокая степень анонимности, обеспечиваемая возможностями глобальной сети Интернет, может существенно облегчить обман предполагаемой жертвы и последующее завладение ее имуществом.

Выбор преступными элементами именно этой разновидности преступлений обусловлен широким распространением мошенничества, многообразием способов его совершения и другими факторами. Мошенники всегда имеют желание максимально обогатиться в минимальные сроки и без финансовых затрат. В связи с этим единственно верным выходом из такой ситуации будет своевременное, постоянное, максимально полное и эффективное информирование о предполагаемой

опасности быть обманутым. Данное информирование должно проходить в рамках правоохранительной деятельности наряду:

1) с эффективным проведением профилактической работы, направленной на предупреждение рассматриваемой категории преступлений;

2) своевременным обнаружением преступлений;

3) качественным расследованием преступлений;

4) информированием населения о результатах деятельности правоохранительных органов по предупреждению и недопущению преступлений;

5) постоянной работой, направленной на более эффективное сотрудничество со средствами массовой информации.

Результаты такой деятельности обеспечат пользователям максимальную безопасность в глобальной сети Интернет.

Информационная среда, в том числе и глобальная сеть Интернет, является сложной технологической системой. Раскрытие преступления как факта его совершения и дальнейшее успешное расследование преступлений в сети Интернет требуют от субъекта расследования не только юридических, но и обширных специальных знаний в области информационно-телекоммуникационных технологий, а также новых алгоритмов действий сотрудников органов внутренних дел.

Раскрытие дистанционных хищений всегда зависит от того, насколько своевременно получена оперативно значимая информация, способа совершения преступления, профессионализма сотрудников и эффективного взаимодействия структурных подразделений Министерства внутренних дел Российской Федерации с другими правоохранительными органами и ведомствами.

В связи с высокими темпами развития общества и расширением сфер его жизнедеятельности все большее внимание уделяется использованию возможностей современного информационного пространства с использованием сети Интернет, количество пользователей этой сферы растет с каждым годом. Отсюда возникают и проблемы, которые носят циклический характер, что создает благоприятную основу для совершения новых видов дистанционных хищений.

В настоящее время, на наш взгляд, можно выделить следующие *основные проблемы, связанные с расследованием различных видов преступлений, совершаемых с использованием возможностей глобальной сети Интернет:*

1) недостаточно высокая степень квалификации лиц, занимающихся расследованием данных преступлений;

2) недостаток практики расследования некоторых видов интернет-хищений;

3) относительно большое количество преступлений, остающихся нераскрытыми;

4) недостаточное количество комментариев специалистов по некоторым проблемным вопросам расследования мошенничеств, совершенных с использованием сети Интернет.

Исходя из вышеизложенного, можно сказать, что борьба с преступлениями, совершаемыми в современном информационном пространстве с использованием сети Интернет, с каждым днем все более усложняется. Ситуации, возникающие в ходе проведения оперативно-розыскных мероприятий и следственных действий, требуют от должностных лиц высокого профессионализма. Для разрешения сложных обстоятельств необходим серьезный подход, и имеющаяся статистика о раскрытии данных видов преступлений говорит о том, что сотрудники органов внутренних дел с ними успешно справляются.

Все чаще через средства массовой информации населению доводятся сведения о новых способах совершения дистанционных хищений, раскрытии преступлений, совершенных организованными преступными группами, и причиненном ущербе. Данная профилактическая работа положительно сказывается на отношении населения к использованию возможностей современных информационных технологий.

Анализируя и обсуждая актуальные вопросы, наиболее часто возникающие в ходе своевременного раскрытия и дальнейшего успешного расследования преступлений, совершаемых в современном информационном пространстве с использованием сети Интернет, необходимо:

1) постоянно повышать свой уровень профессиональных знаний, касающихся непосредственных особенностей организационного, технического и правового обеспечения раскрытия и расследования преступлений;

2) изучать нормы уголовного права, уголовного процесса, новейшие достижения науки криминалистики и других смежных наук, дающие ответы на сложные вопросы, возникающие в ходе раскрытия рассматриваемой категории преступлений;

3) быть в курсе последних законодательных изменений в области банковского, гражданского, информационного, корпоративного права и других смежных отраслей знаний;

4) своевременно получать информацию об организации и технологии обеспечения дистанционного (онлайн) обслуживания, в том числе банковского, что будет способствовать раскрытию преступлений, совершаемых в системе дистанционного банковского обслуживания (ДБО). Выявление, предупреждение, пресечение и раскрытие дистанционных хищений ранее относилось только к компетенции подразделений уголовного розыска. 19 октября 2019 г. создан 6 отдел УУР ГУ МВД России по г. Москве. По результатам работы указанного подразделения выработаны тактика и методика проведения мероприятий по раскрытию дистанционных хищений. Разработаны многочисленные методические

материалы, которые регулярно актуализируются. Неоднократно проводилось обучение личного состава подразделений окружного и районного уровней. Выстроены внутренние и внешние коммуникации, в том числе взаимодействие с различными кредитно-финансовыми организациями и операторами связи, IT-компаниями, а также с иными государственными структурами.

Вместе с тем в соответствии с приказом ГУ МВД России по г. Москве от 10 марта 2023 г. № 93, с 22 мая 2023 г. в структуре аппарата ГУ МВД России по г. Москве в блоке оперативных подразделений создано *Управление по борьбе с противоправным использованием информационно-коммуникационных технологий*, к основным обязанностям которого отнесено выявление, предупреждение, пресечение и раскрытие преступлений, совершаемых с использованием информационно-коммуникационных технологий, в том числе связанных с организованными формами преступности, выявление и установление лиц, их подготавливающих, совершающих или совершивших.

В соответствии с приказом МВД России от 5 апреля 2022 г. № 236 «Об определении полномочий оперативных подразделений органов внутренних дел Российской Федерации по противодействию преступлениям, совершенным с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации», а также приказом ГУ МВД России по г. Москве от 7 июня 2022 г. № 199 «Об определении полномочий оперативных подразделений системы ГУ МВД России по г. Москве по противодействию преступлениям, совершенным с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации», определены 83 состава, относящихся к преступлениям, совершенным с использованием ИКТ или в сфере компьютерной информации, из них к компетенции УБК отнесены 32 состава, УР – 12, ЭБиПК – 9, НОН – 13, ПЭ – 7, ГЗ – 3, СТМ – 7;

5) изучать положения решений пленумов Верховного Суда Российской Федерации о практике рассмотрения уголовных дел по фактам хищения денежных средств в системе дистанционного банковского обслуживания для получения полной информации о ситуации, складывающейся в настоящее время.

Активизировать взаимодействие между регионами Российской Федерации, а также с зарубежными государствами по раскрытию преступлений, совершаемых в современном информационном пространстве с использованием сети Интернет, которое, несомненно, приносит более высокую эффективность в своевременное выявление, предупреждение, раскрытие и успешное расследование преступлений, совершаемых в современном информационном пространстве с использованием сети Интернет.

Рассматриваемые виды преступлений в большинстве случаев имеют транснациональный характер. Зачастую они начинаются в одном регионе того или иного государства, имеют свое продолжение в другой стране, а заканчиваются в третьей. В этих ситуациях разоблачение организованной преступной группы может быть проблематичным. Одной из таких проблем являются различия в национальных уголовных и уголовно-процессуальных законодательствах тех или иных зарубежных государств, что препятствует привлечению к уголовной ответственности лиц, причастных к совершению преступлений.

В связи с изложенным необходимо принять неотложные меры по урегулированию законодательства в сфере противодействия преступлениям, совершаемым в современном информационном пространстве с использованием сети Интернет, на международном уровне.

В настоящее время в реализации вопросов международного сотрудничества налажено взаимопонимание и взаимодействие с такими странами, как Казахстан, Таджикистан, Узбекистан, Киргизия, Белоруссия, Вьетнам, Республика Сербская, Китай, Северная Корея. Необходимо подчеркнуть, что активизируется взаимодействие по решению многих вопросов организационно-служебной деятельности, связанных с регламентом работы Интерпола. Мы надеемся, что в дальнейшем осуществление этой деятельности будет расширено.

Предложенные меры и сделанные выводы по ключевым вопросам раскрытия и расследования дистанционных хищений, по нашему мнению, окажут существенную помощь в борьбе с преступностью.

Представленное научно-практическое пособие позволит сотрудникам органов внутренних дел, призванным по своим функциональным обязанностям раскрывать и расследовать дистанционные хищения, совершаемые с использованием возможностей современного информационного пространства с использованием сети Интернет, в достаточном объеме иметь представление о складывающейся криминогенной обстановке. Собранные наработки, взятые из практической деятельности сотрудников органов внутренних дел, будут способствовать эффективному раскрытию дистанционных хищений, совершаемых в современном информационном пространстве с использованием сети Интернет.

Авторы подготовленного научно-практического пособия абсолютно уверены, что актуальность данного исследования, безусловно, важна и весьма необходима. На современном этапе развития Российской Федерации происходят глубокие политические, социальные, экономические, демографические, правовые и прочие изменения. В связи с этим сотрудники органов внутренних дел, призванные своевременно

раскрывать преступления, совершенные в современном информационном пространстве с использованием сети Интернет, понимают, что добиться высоких результатов в оперативно-служебной деятельности можно лишь тогда, когда будут учитываться определенные положительные тенденции в становлении демократических начал и государственности современной России. Однако социально-экономическая ситуация такова, что общественные отношения не могут эффективно функционировать и многогранно развиваться без должного знания уголовного, уголовно-процессуального, оперативно-розыскного, криминалистического и другого правового научно-исследовательского обеспечения.

Учитывая вышесказанное, необходимо отметить, что сотрудники оперативных структурных подразделений ГУ МВД России по г. Москве уделяют внимание и такому необходимому направлению, как противодействие преступлениям, совершенным в современном информационном пространстве с использованием сети Интернет. Однако в оперативно-служебной деятельности, помимо определенных вытекающих объективных трудностей, есть и другие, субъективные, например недостаточно качественное распределение работы по направлению отдельных видов рассматриваемых преступлений, в связи с чем возникает увеличение сроков разрешения текущих вопросов. Во избежание таких ситуаций руководством ГУ МВД по г. Москве издан приказ от 7 июня 2022 г. № 199 «Об определении полномочий оперативных подразделений системы ГУ МВД России по г. Москве по противодействию преступлениям, совершенным с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации». Данный приказ, естественно, положительно сказывается на решении распределения функциональных обязанностей.

Неотъемлемая составная часть современной профессиональной службы в органах внутренних дел обязывает ее сотрудников своевременно выявлять, пресекать, предупреждать, раскрывать и расследовать подготавливаемые или совершенные преступления. Для реализации поставленных задач, достижения положительных результатов и высоких показателей сотрудникам оперативных подразделений и следственных органов ГУ МВД России по г. Москве необходимо получение специальных знаний в области оперативно-розыскной деятельности, уголовного процесса, криминалистики, судебной экспертизы, и в зависимости от возникающей ситуации – знание многих других вопросов.

Криминогенная ситуация в стране продолжает оставаться достаточно сложной. В связи с этим практические сотрудники, обладающие навыками своевременно раскрывать и расследовать различного рода и вида преступления, совершаемые в новых современных условиях, остро нуждаются и в необходимых научно-исследовательских разработках. Их содержание

позволит преумножить и систематизировать сведения, что, безусловно, сыграет положительную роль в борьбе с преступностью.

Научно-исследовательская деятельность стала неотъемлемой частью работы правоохранительных органов, а XXI век привнес новые вызовы, такие как киберпреступность, терроризм и преступления, связанные с незаконным оборотом наркотиков, способы совершения которых стали носить более изощренный характер.

Для этого сотрудники органов внутренних дел постоянно должны быть нацелены на повышение своего профессионализма.

В целях разрешения имеющихся проблем, связанных с оперативно-розыскным обеспечением, направленным на своевременное раскрытие и успешное расследование преступлений, научно-исследовательская работа становится вдвойне актуальной с позиций удовлетворения требований общества в необходимости применения адекватных мер борьбы с преступностью.

Важно понимать и необходимо знать, что научно-исследовательская работа, ее содержание или накопленная в ней информация преследует одну главную цель – обеспечение комплексного механизма, направленного на своевременное раскрытие и предотвращение преступлений. Данный механизм должен содержать в себе многогранный комплекс, включающий в себя следующее:

1. В зависимости от ситуации – проведение необходимых оперативно-розыскных мероприятий.

2. При возбужденном уголовном деле в стадии предварительного расследования – проведение следственных действий, направленных на своевременное выявление, пресечение, предотвращение, раскрытие и успешное расследование преступлений.

3. При необходимости – проведение оперативно-розыскных мероприятий и в период, когда ведется судебное заседание, слушание уголовного дела, вынесение судебного приговора и, если ситуация требует, то и после него.

Как выше было сказано, в современном обществе преступность является одной из наиболее острых социальных проблем, требующих комплексного подхода к своему решению, и в этом случае особое место занимает научно-исследовательская деятельность, способствующая раскрытию и расследованию преступлений. Данные исследования направлены не только на изучение преступных явлений, но и на разработку новых методов и современных технологий, которые помогают правоохранительным органам эффективно выполнять свои функции.

Изучение и последующее применение современных методов научного анализа и новых криминалистических технологий способствуют повышению эффективности работы сотрудников правоохранительных органов, также укрепляют общественное доверие к правоохранительной системе.

Научно-исследовательская работа, проводимая в органах внутренних дел, направлена на решение конкретных задач, стоящих перед МВД России.

Разработки в области компьютерной криминалистики, оперативно-розыскной деятельности могут помочь в анализе больших объемов данных при расследовании преступлений, совершаемых в современном информационном пространстве с использованием сети Интернет. Установление связи между разными данными, полученными в ходе расследования, может значительно ускорить процесс выявления преступника. Кроме того, применение таких технологий, как видеонаблюдение и системы распознавания лиц, стало возможным именно благодаря интенсивным научным исследованиям, которые направлены на улучшение методов идентификации личности.

В завершение научно-практического исследования по теме «Особенности раскрытия преступлений, совершаемых в современном информационном пространстве с использованием сети Интернет», хочется привести актуальную фразу, высказанную заместителем руководителя Главного управления криминалистики Следственного комитета Российской Федерации – руководителем технико-криминалистического управления, генерал-майором юстиции И. А. Стрельцовым: «В современных условиях оперативный сотрудник в тесном взаимодействии со следователем обязан обладать не только глубокими юридическими знаниями, но и высокими цифровыми компетенциями. Особое значение приобретает подготовка специалистов нового поколения, способных эффективно работать в единой национальной системе данных, а также профессионально использовать передаваемые технологии анализа больших данных, искусственного интеллекта и цифровой экспертизы».

Проанализировав преступления, совершаемые в современном информационном пространстве с использованием сети Интернет, авторы научно-практического пособия считают целесообразным **внести дополнение в Концепцию государственной системы противодействия противоправным деяниям, совершаемым с использованием информационно-коммуникационных технологий**, утвержденную распоряжением Правительства Российской Федерации 30 декабря 2024 г. № 4154-р⁴⁰, в гл. I «Общие положе-

⁴⁰ Об утверждении Концепции государственной системы противодействия противоправным деяниям, совершаемым с использованием информационно-коммуникационных технологий: распоряжение Правительства Российской Федерации

ния» ввести понятие «противоправные деяния, совершенные с использованием информационно-коммуникационных технологий». Далее по тексту заменить словосочетание «противоправные деяния» на слово «киберпреступления».

Авторский коллектив научно-практического пособия выражают глубокую признательность и благодарность в оказании помощи по сбору материалов профессорско-преподавательскому составу кафедры информационных технологий Академии управления МВД России, сотрудникам Управления уголовного розыска и Управления по борьбе с противоправным использованием информационно-коммуникационных технологий МВД России по г. Москве, а также слушателям, в разные периоды проходившим обучение на кафедре оперативно-технических мероприятий органов внутренних дел ВШП МВД России.

Литература

1. **Российская Федерация. Законы.** Конституция Российской Федерации : принята всенародным голосованием 12 декабря 1993 г. (с изм., одобренными в ходе общероссийского голосования 1 июля 2020 г.) // СПС «КонсультантПлюс» : [сайт]. – URL: https://www.consultant.ru/document/cons_doc_LAW_28399/ (дата обращения: 25.12.2025).
2. **Российская Федерация. Законы.** Уголовный кодекс Российской Федерации : Федеральный закон от 13 июня 1996 г. № 63-ФЗ // СПС «КонсультантПлюс» : [сайт]. – URL: https://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения: 19.12.2025).
3. **Российская Федерация. Законы.** Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ (ред. от 8 марта 2026 г.) // СПС «КонсультантПлюс» : [сайт]. – URL: https://www.consultant.ru/document/cons_doc_LAW_34481/ (дата обращения: 15.03.2026).
4. **Российская Федерация. Законы.** О государственной тайне : Закон Российской Федерации от 21 июля 1993 г. № 5485-1 // СПС «КонсультантПлюс» : [сайт]. – URL: https://www.consultant.ru/document/cons_doc_LAW_2481/ (дата обращения: 10.09.2025).
5. **Российская Федерация. Законы.** Об оперативно-розыскной деятельности : Федеральный закон от 12 августа 1995 г. № 144-ФЗ // СПС «КонсультантПлюс» : [сайт]. – URL: https://www.consultant.ru/document/cons_doc_LAW_7519/ (дата обращения: 10.09.2025).
6. **Российская Федерация. Законы.** О Центральном банке Российской Федерации (Банке России) : Федеральный закон от 10 июля 2002 г. № 86-ФЗ // СПС «КонсультантПлюс» : [сайт]. – URL: https://www.consultant.ru/document/cons_doc_LAW_37570/ (дата обращения: 10.09.2025).
7. **Российская Федерация. Законы.** О связи : Федеральный закон от 7 июля 2003 г. № 126-ФЗ // СПС «КонсультантПлюс»: [сайт]. – URL: https://www.consultant.ru/document/cons_doc_LAW_43224/ (дата обращения: 25.12.2025).
8. **Российская Федерация. Законы.** О коммерческой тайне : Федеральный закон от 29 июля 2004 г. № 98-ФЗ // СПС «КонсультантПлюс»: [сайт]. – URL: https://www.consultant.ru/document/cons_doc_LAW_48699/ (дата обращения: 25.12.2025).

9. **Российская Федерация. Законы.** Об информации, информационных технологиях и о защите информации : Федеральный закон от 27 июля 2006 г. № 149-ФЗ // СПС «КонсультантПлюс»: [сайт]. – URL: https://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 25.12.2025).

10. **Российская Федерация. Президент.** О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы : Указ Президента Российской Федерации от 9 мая 2017 г. № 203 // Информационно-правовой портал «Гарант.Ру». – URL: <https://www.garant.ru/products/ipo/prime/doc/71570570/> (дата обращения: 12.09.2025).

11. **Российская Федерация. Правительство.** Об утверждении Положения о защите информации в платежной системе : постановление Правительства Российской Федерации от 13 июня 2012 г. № 584 // СПС «КонсультантПлюс» : [сайт]. – URL: https://www.consultant.ru/document/cons_doc_LAW_131173/05c3f1053d0d0a27e491cc7c3a0d509157c92a4f/ (дата обращения: 12.09.2025).

12. Об отчетности по обеспечению защиты информации при осуществлении переводов денежных средств операторов платежных систем, операторов услуг платежной инфраструктуры, операторов по переводу денежных средств : указание Банка России от 9 июня 2012 г. № 2831-У // СПС «КонсультантПлюс» : [сайт]. – URL: https://www.consultant.ru/document/cons_doc_LAW_131471/251f7ac207ca304c6331640eb36b162351c24684/ (дата обращения: 10.09.2025).

13. О рекомендациях по организации применения средств защиты от вредоносного кода при осуществлении банковской деятельности : письмо Банка России от 24 марта 2014 г. № 49-т // Информационно-правовой портал «Гарант.Ру». – URL: <https://www.garant.ru/products/ipo/prime/doc/70526030/> (дата обращения: 10.09.2025).

14. **Российская Федерация.** Об утверждении типовых Требований к плану мероприятий по внедрению технических средств, обеспечивающих оперативно-розыскную деятельность : приказ Минцифры России, ФСБ России № 245/127 от 28 марта 2022 г. // Информационно-правовой портал «Гарант. Ру». – URL: <https://www.garant.ru/products/ipo/prime/doc/404991787/> (дата обращения: 10.09.2025).

15. **Российская Федерация.** Об утверждении Инструкции о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд : приказ МВД России, МО России, ФСБ России, ФСО России, ФТС России, СВР России, ФСИН России, ФСКН России, СК России от 27 сентября 2013 г. № 776/703/5 09/507/1820/42/535/398/68 // Информационно-правовое

обеспечение «Гарант» : [сайт]. – URL: <https://base.garant.ru/70531824/> (дата обращения: 25.12.2025).

16. Состояние преступности за 2008–2012 гг. : сборники ФКУ «ГИАЦ МВД России».

17. **Акопов, Г. Л.** Интернет и политика. Модернизация политической системы на основе инновационных политических интернет-коммуникаций / Г. Л. Акопов. – Москва : Кнорус, 2014.

18. **Алескеров, В. И.** Уголовно-правовая и криминалистическая характеристика современных видов преступлений в сфере компьютерной информации : лекция / В. И. Алескеров, И. А. Максименко. – Домодедово : ВИПК МВД России, 2011.

19. **Алескеров, В. И.** Преступления, совершаемые в телекоммуникационных сетях, как разновидность преступлений в сфере компьютерной информации : аналитический сборник / В. И. Алескеров, Ф. А. Куц. – Домодедово : ВИПК МВД России, 2014.

20. **Алескеров, В. И.** Раскрытие преступлений в сфере телекоммуникаций и компьютерной информации : учебно-практическое пособие / В. И. Алескеров, О. Н. Колокольчикова. – Домодедово : ВИПК МВД России, 2018.

21. **Алескеров, В. И.** Особенности раскрытия преступлений в сфере компьютерной информации : учебно-практическое пособие / В. И. Алескеров, О. Н. Колокольчикова. – Домодедово : ВИПК МВД России, 2015.

22. **Алескеров, В. И.** Раскрытие преступлений в сфере телекоммуникаций и компьютерной информации : учебно-практическое пособие / В. И. Алескеров, О. Н. Колокольчикова. – Домодедово : ВИПК МВД России, 2018.

23. **Алескеров, В. И.** Выявление и раскрытие преступлений экстремистской и террористической направленности, совершаемых с использованием сферы телекоммуникаций и компьютерной информации : учебно-практическое пособие / В. И. Алескеров, О. Н. Колокольчикова, А. И. Федоткин. – Домодедово : ВИПК МВД России, 2018.

24. **Алескеров, В. И.** Раскрытие преступлений в системе дистанционного банковского обслуживания : учебно-практическое пособие / В. И. Алескеров, О. Н. Колокольчикова, Л. В. Василенко. – Домодедово : ВИПК МВД России, 2020.

25. **Алескеров, В. И.** Сфера телекоммуникаций и компьютерной информации как платформа для совершения современных видов преступлений : учебно-практическое пособие / В. И. Алескеров, О. Н. Колокольчикова, Л. В. Василенко. – Домодедово : ВИПК МВД России, 2022.

26. **Алескеров, В. И.** Сфера телекоммуникаций и компьютерной информации как платформа для совершения современных видов преступлений : учебно-практическое пособие / В. И. Алескеров, О. Н. Колокольчикова, Л. В. Василенко; под общ. ред. М. Ю. Литвинова. – Домодедово : ВИПК МВД России, 2024.

27. **Алескеров, В. И.** Раскрытие дистанционных хищений, совершаемых с использованием IT-технологий: научно-практическое пособие / В. И. Алескеров, О. Н. Колокольчикова, Е. В. Маркелова [и др.]; под общ. ред. М. Ю. Литвинова. – Домодедово : ВИПК МВД России, 2024.

28. **Литвинов, М. Ю.** Противодействие современным видам преступлений, совершаемых в условиях цифровизации : учебно-практическое пособие : в 3 частях / М. Ю. Литвинов, В. И. Алескеров, О. Н. Колокольчикова. – Домодедово : ВИПК МВД России, 2025.

29. **Алпатов, А. С.** Мошенничество и причинение имущественного ущерба путем обмана или злоупотребления доверием / А. С. Алпатов // Трибуна молодого ученого. – 2016. – № 2.

30. **Баулин, В. В.** Методы совершения хищений денежных средств через систему дистанционного банковского обслуживания / В. В. Баулин, Д. Волков, В. В. Баранов, А. А. Рыжков // Сборник трудов XXIII Всероссийской конференции «Информатизация и информационная безопасность правоохранительных органов». – Москва, 2014.

31. **Дуленко, В. А.** Преступление в сфере высоких технологий : учебное пособие / В. А. Дуленко, Р. Р. Мамлеев, В. А. Пестриков. – Москва : ЦОКР МВД России, 2010.

32. **Еферин, В. П.** Организация деятельности территориальных органов МВД России на районном уровне по противодействию терроризму и экстремизму : учебное пособие / В. П. Еферин, Ю. П. Хорькин. – Домодедово : ВИПК МВД России, 2014.

33. Историческая и социально-образовательная мысль // Всероссийский научный журнал. – 2014. – № 4 (26).

34. Комментарий к Уголовному кодексу Российской Федерации (постатейный) / отв. ред. А. И. Рарога. – 12-е изд., перераб. и доп. – Москва : «Проспект», 2017.

35. **Кочои, С.** Ответственность за неправомерный доступ к компьютерной информации / С. Кочои, Д. Савельев // Российская юстиция. – 1999. – № 1.

36. **Крылов, В. В.** Информация как элемент криминальной деятельности / В. В. Крылов // Российская юстиция. – № 5. – 2000.

37. **Маторин, М. А.** Актуальные вопросы формирования правовой системы противодействия терроризму / М. А. Маторин // *Оперативник (сыщик)*. – 2014. – № 2 (39).
38. **Медведев, В. Н.** Правовое регулирование снятия информации с технических каналов связи в оперативно-розыскной деятельности : диссертация ... кандидата юридических наук. – Санкт-Петербург : Санкт-Петербургский университет, 2003.
39. **Мельников, Д. А.** Организация и обеспечение безопасности информационно-телекоммуникационных сетей и систем : учебник / Д. А. Мельников. – Москва : ИД КДУ, 2015.
40. **Мирошников, Б. Н.** Сетевой фактор. Интернет и общество / Б. Н. Мирошников. – Москва : Кучково поле, 2015.
41. **Россинская, Е. Р.** Судебная экспертиза в гражданском, административном и уголовном процессе / Е. Р. Россинская. – Москва : Норма, 2020.
42. Сайт Центра исследований компьютерной преступности. – URL: <http://www.crime-research.ru> (дата обращения: 20.01.2018).
43. **Сейджман, М.** Сетевые структуры терроризма / М. Сейджман. – Москва : Идея-Пресс, 2008.
44. **Синякин, И. И.** Терроризм с использованием оружия массового уничтожения: международно-правовые вопросы противодействия : монография / И. И. Синякин. – Москва : Норма, 2012.
45. **Сорокин, А. В.** Судебная практика по делам о преступлениях в сфере компьютерной информации. – URL: http://www.zaural.ru/procur/my_page.htm (дата обращения: 20.01.2018).
46. Теория оперативно-розыскной деятельности : учебник / под ред. К. К. Горяинова, В. С. Овчинского, Г. К. Синилова. – 3-е изд., перераб. и доп. – Москва : ИНФРА-М, 2014.
47. Терроризм в современном мире / под ред. В. Л. Шульца. – 2-е изд. – Центр исследования проблем безопасности РАН. – Москва : Наука, 2011.
48. **Тищенко, В. И.** Сетевые взаимодействия. Предмет исследования и объект моделирования / В. И. Тищенко, Т. И. Жуков, Ю. С. Попков. – Москва : Ленанд, 2014.
49. **Ткаченко, В. В.** Российский терроризм. Проблемы уголовной ответственности : монография / В. В. Ткаченко. – Москва : ИНФРА-М, 2014.
50. **Троицкий, С. В.** Международно-правовые формы сотрудничества государств по противодействию терроризму / С. В. Троицкий // *Государство и право*. – 2014. – № 2.
51. **Ульянова, В. В.** Проблемы реализации уголовной ответственности за содействие террористической деятельности в форме

финансирования терроризма / В. В. Ульянова // Актуальные проблемы российского права. – 2014. – № 3.

52. **Фатьянов, А. А.** Правовое обеспечение безопасности информации в Российской Федерации : учебное пособие / А. А. Фатьянов. – Москва, 2001.

53. **Чекунов, И. Г.** Современные киберугрозы. Уголовно-правовая и криминологическая классификация и квалификация киберпреступлений / И. Г. Чекунов // Право и кибербезопасность. – 2012. – № 1.

54. **Шаталов, А. С.** Криминалистические алгоритмы и программы. Теория. Проблемы. Прикладные аспекты / А. С. Шаталов. – Москва : Лига Разум, 2000.

55. **Шаталов, А. С.** Уголовно-процессуальное право Российской Федерации : академический курс по направлению «Юриспруденция» / А. С. Шаталов, А. А. Крымов. – Москва : Проспект, 2018.

56. **Шаталов, А. С.** Уголовно-процессуальный кодекс Российской Федерации в схемах : учебное пособие / А. С. Шаталов. – Москва : Проспект, 2021.

57. **Шеннон, К.** Работы по теории информации и кибернетике / К. Шеннон. – Москва, 1963.

58. **Шмонин, А. В.** Организация выявления и раскрытия хищений денежных средств с использованием дистанционного банковского обслуживания / А. В. Шмонин // Сборник трудов XXIII Всероссийской конференции «Информатизация и информационная безопасность правоохранительных органов». – Москва, 2014.

Научное издание

Алескеров Вагиф Исмаилович,
кандидат юридических наук, доцент
Баранов Владимир Владимирович
кандидат юридических наук
Колокольчикова Ольга Николаевна
Кононенко Антон Викторович
Косцов Алексей Олегович
Маркелова Елена Владимировна

**ОСОБЕННОСТИ РАСКРЫТИЯ ПРЕСТУПЛЕНИЙ,
СОВЕРШАЕМЫХ В СОВРЕМЕННОМ
ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ
С ИСПОЛЬЗОВАНИЕМ СЕТИ ИНТЕРНЕТ**

Редактирование А. В. Николаева
Техническое редактирование Е. В. Бухарина
Подписано в печать 30.03.2026.
Формат 60х84 1/16. Объем 7,5 уч.-изд. л.
Тираж 44 экз. Заказ 02/26. Цена договорная.

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