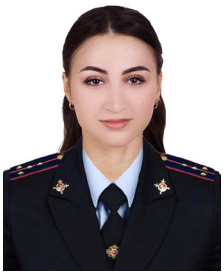
УДК 343.98



Нина Игоревна СТАРОСТЕНКО,
старший преподаватель кафедры криминалистики
Краснодарского университета МВД России,
кандидат юридических наук
ninastarostenko@bk.ru

Олег Александрович СТАРОСТЕНКО,
старший преподаватель кафедры
оперативно-разыскной деятельности в ОВД
Краснодарского университета МВД России,
кандидат юридических наук
olegstaros94@gmail.com

КРИМИНАЛИСТИЧЕСКАЯ ХАРАКТЕРИСТИКА ОСНОВНЫХ СПОСОБОВ ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ ОРГАНИЗОВАННЫМИ ПРЕСТУПНЫМИ ФОРМИРОВАНИЯМИ С ПРИМЕНЕНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

CRIMINALISTIC CHARACTERISTICS OF THE MAIN METHODS OF CRIMES COMMITTED BY ORGANIZED CRIMINAL GROUPS USING INFORMATION AND TELECOMMUNICATION TECHNOLOGIES

В статье представлена криминалистическая характеристика способов преступлений, совершаемых организованными преступными формированиями с применением информационно-телекоммуникационных технологий. Исследование основано на всеобщем диалектико-материалистическом методе познания закономерностей системы действий участников преступных формирований при совершении преступлений с применением информационно-телекоммуникационных технологий. Анализ способов совершения указанных преступлений позволил выявить их закономерные связи с другими элементами криминалистической характеристики, в частности с личностью преступника, личностью потерпевшего, механизмом следообразования и др. Определена позиция относительно типичных следов данной противоправной деятельности. Криминалистические знания о структурных элементах способов совершения преступлений организованными преступными формированиями с применением информационно-телекоммуникационных технологий могут быть использованы при расследовании преступлений обозначенной категории в процессе построения следственных версий, а также учитываться для эффективного планирования комплекса оперативно-розыскных мероприятий и следственных действий.

The article presents a criminalistic description of the methods of crimes committed by organized criminal groups using information and telecommunication technologies. The research is based on a universal dialectical-materialistic method of understanding the patterns of the system of actions of participants in criminal groups when committing crimes using information and telecommunication technologies. The analysis of the methods of committing these crimes allows revealing their natural connections with other elements of forensic characteristics, in particular with the personality of the criminal, the personality of the victim, the mechanism of trace formation, etc. The position regarding the typical traces of this illegal activity is determined. Forensic knowledge about the structural elements of the methods of committing crimes by organized criminal groups using information and telecommunication technologies can be used in the investigation of crimes of the designated category in the process of building lines of investigation, as well as be taken into account for effective planning of a complex of operational search measures and investigative actions.

Ключевые слова: криминалистика, преступления, информационно-телекоммуникационные технологии, способы совершения преступлений, сокрытие преступлений, организованные преступные формирования.

Keywords: *forensics, crimes, information and telecommunication technologies, methods of committing crimes, concealment of crimes, organized criminal groups.*

В настоящее время деяния, которые совершаются преступными формированиями (группами, сообществами), определяются в качестве узлового элемента преступности, требующего активного противодействия. Так, на расширенном заседании Коллегии МВД России 2 апреля 2024 г. В.В. Путин уделил особое внимание таким приоритетам, как действия МВД по нейтрализации организованной преступности, поскольку такие группировки часто носят трансграничный характер, действуют «рука об руку» с зарубежными спецслужбами, эмиссарами международных радикальных, экстремистских структур. Подобные криминальные сообщества завязаны на торговлю людьми, незаконный оборот оружия, наркотрафик[1]. Кроме того, среди преступлений, совершенных организованными преступными формированиями, отмечаются киберхищения, незаконный оборот боеприпасов, взрывных устройств и веществ, неправомерный доступ к компьютерной информации, распространение противоправной информации (клеветы, материалов порнографического характера, материалов, возбуждающих межнациональную и межрелигиозную вражду, и т.д.) через Интернет, а также вредоносное вмешательство через компьютерные сети в работу различных систем, создание, использование и распространение вредоносных компьютерных программ, нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

По данным официальной статистики МВД России, в 2024 г. организованными группами или преступными сообществами совершены 36,1 тыс. тяжких и особо тяжких преступлений (+17,1%), причем их удельный вес в общем числе расследованных преступлений этих категорий увеличился с 11,6% в 2023 г. до 13,8%[2].

Преступления подобного рода, по мнению ряда ученых, несомненно, обладают высокой латентностью, что правомерно рассматривать как результат их активного противодействия деятельности правоохранительных органов, в том числе направленной на раскрытие и расследование преступлений [12, с. 490].

С учетом изложенного, следует констатировать, что разработка научных подходов методики расследования преступлений, совершаемых преступными формированиями (группами, сообществами) в сфере информационно-телекоммуникационных технологий, обусловлена потребностями следственной практики в разработке усовершенствованных приемов, средств, методов и практических рекомендаций по выявлению, раскрытию и расследованию данных преступлений.

Актуальность указанной темы подтверждается нарастающей общественной опасностью преступлений, совершаемых организованными преступными формированиями, нереализованными возможностями правоохранительных органов в их раскрытии и расследовании, что особенно проявляется в части научно-технического, оперативно-розыскного и информационного обеспечения их деятельности.

Исследованию проблем, связанных с раскрытием и расследованием преступлений, совершаемых в рамках организованной преступной деятельности, посвящены работы А.М. Каминского [3], В.И. Комиссарова [5], В.И. Куликова [6], Д.Н. Лозовского [7], Я.М. Мазунина [8], А.Л. Осипенко [9], А.И. Романова [10], И.В. Тишутиной [12], Н.П. Яблокова [14] и других.

1 URL: http://www.kremlin.ru/events/president/transcripts/deliberations/73770 (дата обращения: 19.11.2024).
2 URL: https://мвд.рф/reports/item/60248328/ (дата обращения : 25.03.2025).

Н.П. Яблоков определял организованную преступность как единую системную совокупность разных видов профессионально совершаемых преступлений в виде постоянного промысла усилиями лиц, объединенных в специально созданные устойчивые, хорошо организованные, законспирированные и защищенные от разоблачения формирования. По мнению автора, такие формирования могут существовать независимо или являться структурными частями еще более сложной преступной системы межрегионального или транснационального уровня [14].

Особое место в работе следователя занимает деятельность по изучению методик расследования преступлений отдельных видов, которые содержат определенные криминалистические рекомендации и могут помочь правоприменителю эффективно организовать и спланировать свою работу. При этом фундаментальную роль в структуре каждой отдельной методики расследования преступления играет его криминалистическая характеристика, поскольку она используется при анализе особенностей преступности, свойственных конкретной группе противоправных деяний, разработке общих и частных версий, а также при производстве отдельных следственных действий.

При исследовании определенного вида преступности «внимание криминалистов привлекает преимущественно механизм преступления и такая его составляющая, как способы подготовки, совершения и сокрытия преступлений. Без их знания, без знания тех признаков, которые указывают на их использование в данном случае, невозможно расследовать преступление. Недаром в криминалистике существует принцип: «От способа совершения преступления – к способу его выявления и раскрытия» [1, с. 685]. Именно поэтому данные о таких способах служат одной из исходных посылок при разработке частных криминалистических методик. Более того, подобный подход к преступлению дает возможность точнее представить себе развитие и формирование механизма хищений изучаемого вида.

В научной литературе существуют различные подходы к определению способа совершения преступления. Так, А.Н. Колесниченко под способом совершения преступления понимает образ действий преступника, выражающийся в определенной последовательности, сочетании отдельных действий, приемов, применяемых субъектом. С точки зрения автора, способ приготовления к совершению преступления, способ совершения самого преступления и способ его сокрытия следует рассматривать отдельно [4, с. 18].

Г.Г. Зуйков рассматривает способ совершения преступления как систему действий по подготовке, совершению и сокрытию преступления, детерминированных условиями внешней среды и психофизическими свойствами личности, могущих быть связанными с избирательным использованием соответствующих орудий или средств в условии места и времени [2, с. 10].

Особого внимания заслуживает позиция Н.П. Яблокова, который под способом совершения преступления в криминалистическом смысле понимает объективно и субъективно обусловленную систему поведения субъекта до, в момент и после совершения им преступления, оставляющую вовне различного рода характерные следы, позволяющие с помощью криминалистических приемов и средств получить представление о сути происшедшего, своеобразии преступного поведения правонарушителя, его отдельных личностных данных и, соответственно, определить наиболее оптимальные методы решения задач раскрытия преступления [15, с. 210-300].

Отметим, что способы совершения преступлений организованными преступными формированиями являются полноструктурными, поскольку они включают в себя подготовку, непосредственное совершение и сокрытие следов преступления.

Преступные формирования при реализации криминальных целей осуществляют тщательную и планомерную подготовку, подразумевающую разнообразие современных методов и подходов, необходимых для выполнения непосредственных действий.

Рассмотрим некоторые из них.

Приискание информации о потенциальной жертве или объекте преступного посягательства. Данная деятельность подразумевает предварительный сбор и анализ сведений о предполагаемом объекте для воздействия. В таких случаях преступники могут использовать возможности технологий искусственного интеллекта, таких как OSINT-технологий, а также осуществлять сбор информации со страниц социальных сетей, публичных баз данных и форумов. Далее собранная информация интерпретируется под преступные цели.

Создание сайтов, алгоритмов и приискание инструментов, необходимых для совершения преступлений. К таким инструментам можно отнести вредоносные программы (вирусы, трояны, шпионские программы), фишинговые сайты, программы для удаленного администрирования.

Ученые и правоприменители все чаще отмечают негативную тенденцию применения злоумышленниками технологий искусственного интеллекта в преступной деятельности, например Chat GPT. Так, эксперты предполагают, что в 2025 г. возрастет количество преступлений с использованием данной технологии. По словам IT-эксперта Д. Штаненко, основная опасность заключается в том, что пользователи могут использовать чат-бота для создания инструкции по изготовлению оружия, взрывчатых устройств, химических соединений, чтобы использовать их в террористических целях[1].

Обеспечение анонимности действий. Преступники могут прибегать к самым различным способам обеспечения анонимности в сети Интернет. Р.А. Усманов подразделяет такие способы на две группы: 1) без использования специального программного или аппаратного обеспечения (использование «ника», вымышленного имени, чужого компьютера, изменение вручную MAC-адреса сетевого устройства, IP-адреса компьютера) 2) с использованием специального программного или аппаратного обеспечения [13]. Подчеркнем, что участники организованных преступных групп чаще всего прибегают ко второму способу, а именно использованию различных анонимайзеров, прокси-сервисов, специальных браузеров (например, Tor Browser) для сокрытия преступных действий в сети, своего местоположения, IP-адреса компьютерного устройства, сохраняя при этом анонимность. Необходимо отметить, что такие сервисы являются посредниками между преступником и интересующим его ресурсом, например, Даркнетом, теневым сегментом Интернета, который скрыт из общего доступа. Подобные инструменты в руках злоумышленников существенно усложняют последующую идентификацию участников преступных формирований правоохранительными органами, поскольку серверы указанных сервисов, обеспечивающих соединение, как правило, располагаются за пределами территории Российской Федерации.

В преступной деятельности организованные преступные формирования используют различные способы и методы.

К основным способам отнесем:

– *преступные действия в сфере компьютерной информации*. Данный способ совершения преступлений предусматривает деятельность, направленную на незаконный доступ и последующее использование при совершении преступлений банковских сведений, персональных данных, паролей и логинов, а также другой информации о потенциальной жертве. Как правило, данный способ реализуется злоумышленниками путем создания фишинговых сайтов, выполнения рассылки фишинговых писем, осуществления звонков жертвам с применением средств мобильной или голосовой связи, установки «вирусов», «червей» или шпионского программного обеспечения на устройства жертв. При этом преступники либо продают полученную информацию, либо самостоятельно исполь-

1 Эксперты предполагают, что в 2025 году возрастет количество преступлений с использованием ИИ. URL: https://www.seonews.ru/events/eksperty-predpolagayut-chto-v-2025-godu-vozrastet-kolichestvo-prestupleniy-s-ispolzovaniem-ii/?utm_source=yandex.ru&utm_medium=organic&utm_campaign=yandex.ru&utm_referrer=yandex.ru (дата обращения: 15.01.2025).

зуют ее в мошеннических целях;

– *мошеннические действия с применением методов социальной инженерии*. Под методами социальной инженерии следует понимать совокупность психологических приемов, технических действий по применению программных средств, технологий в процессе подготовки, непосредственного совершения и сокрытия преступления, направленных на оказание психологического воздействия на сознание и поведение людей, создание условий, необходимых для дистанционного хищения чужого имущества. Следует акцентировать внимание на том, что применение указанных методов позволяет преступнику создать такие условия, при которых жертва: 1) *самостоятельно* выполняет перевод денежных средств на определенный банковский счет, принадлежащий третьим лицам, либо под контролем преступников совершает иные финансовые операции; 2) *добровольно* предоставляет преступникам удаленный доступ или управление электронным устройством либо передает код из SMS-сообщений от банка, подтверждающий финансовую операцию, реквизиты банковской карты, в том числе CVC2/CVV2-код, логины и пароли от сервиса дистанционного банковского обслуживания, а также иную информацию, необходимую для хищения чужого имущества. Методы социальной инженерии включают в себя психологические приемы манипуляции, связанные с использованием специально подготовленного сценария или текста, предусматривающего исполнение определенной роли при осуществлении преступных действий в целях оказания воздействия на психоэмоциональное состояние жертвы для изменения ее восприятия и убеждения в необходимости срочного принятия решения в ограниченный период времени, технологические приемы манипуляции, направленные на создание поддельного интернет-сайта, фишинговой ссылки и (или) использование определенных программных средств для дистанционного воздействия на жертву, обеспечивающих сокрытие преступных действий («deepfake»-технологии, программы для изменения голоса, подмены номера телефона, предоставления удаленного доступа к компьютерному или мобильному устройству, вредоносное программное обеспечение и др.) [подр.: 11];

– *преступные сделки в сети Интернет*. Данный способ охватывает деятельность участников преступных группировок, связанную с незаконным оборотом наркотических средств, оружия и боеприпасов, а также других объектов, запрещенных к обращению в гражданском обороте.

При осуществлении преступной деятельности подобным способом используются специальные электронные платформы, расположенные в Даркнете, а также социальные сети, мессенджеры и специализированные форумы, где обсуждаются вопросы, связанные с реализацией указанных товаров и услуг;

– *преступления, связанные с размещением в сети Интернет противоправной информации*. К данному способу совершения преступлений необходимо отнести действия преступников, связанные с размещением в сети Интернет инструкций по изготовлению наркотических средств, взрывных устройств, публикацией недостоверной информации о человеке или организации, которая может нанести ущерб репутации или информации с целью получения финансовой прибыли, контента, разжигающего ненависть расовой, этнической, религиозной или иной принадлежности, а также распространением детской порнографии, нарушением авторских прав и др.

Сокрытие следов преступной деятельности. Противодействие расследованию преступлений со стороны участников преступных формирований может проявляться в различных формах и включать в себя множество стратегий. Назовем некоторые из них.

Сокрытие движения денежных средств, добытых преступным путем, по банковским счетам, а также их легализация. Здесь следует отметить процессы, направленные на сокрытие незаконного источника дохода, включая использования подставных компаний, сложных финансовых операций с криптовалютой, а также многократный перевод денежных средств на различные подконтрольные третьим лицам счета, с вовлечением в эту деятельность дропов.

Использование современных технологий, таких как шифрование, анонимайзеры на всех этапах совершения преступлений. Использование подобных технологий дает преступникам возможность скрывать свою личность, местоположение и содержание передаваемой информации, что создает дополнительные сложности для правоохранительных органов при сборе доказательств и идентификации виновных лиц.

Размещение сведений об объектах, запрещенных в гражданском обороте в теневой сети Интернета. Подобный способ сокрытия позволяет обмениваться информацией, координировать действия и реализовывать запрещенные товары и услуги, минимизируя риск обнаружения и привлечения к ответственности.

Уничтожение информации о жертвах преступления. Участники преступных формирований, совершающие преступления рассматриваемого вида, могут использовать различные способы уничтожения информации о жертвах после совершения преступления. К таким способам можно отнести форматирование используемой информации (физическое удаление данных о жертве), шифрование данных для усложнения их восстановления, удаление метаданных, содержащих сведения о действиях злоумышленников в системе, применение вредоносного программного обеспечения, настроенного под удаление данных, использование техник «стирания цифрового следа» (очистка цифровой истории).

Фальсификация сведений в сети. Одним из основных методов является создание фальшивых аккаунтов и веб-ресурсов, которые используются для распространения дезинформации, вербовки новых членов и координации преступной деятельности.

Создание «эшелонов» внутри организации. Данный способ сокрытия характеризуется действиями, направленными на создание структурированной иерархии, распределения ролей, а также обеспечения безопасности.

Практически в каждом организованном преступном формировании, состоящем из нескольких десятков активных членов, можно выделить три уровня структурных звеньев. В данной структуре могут выделяться лидеры (верхний эшелон), которые принимают основные решения группы. При этом они часто могут оставаться неизвестными для иных участников группы. Далее в иерархии выделяются управляющие, которые отвечают за координацию и решение ключевых преступных целей. И исполнители, рядовые участники преступных групп, которые непосредственно совершают преступления. Также можно выделить «внешних участников преступных формирований». К подобным субъектам относятся коррумпированные чиновники, сотрудники правоохранительных органов, участники бизнес-структур и других лиц, оказывающих помощь в сокрытии следов преступной деятельности или влиянии на ход расследования.

Особенно подчеркнем, что каждые из указанных видов могут комбинироваться, создавая сложные схемы преступной деятельности, влияющих на успешное раскрытие и расследование преступлений изучаемого вида.

Кроме того, преступные группы, систематически совершающие дистанционные хищения, создают специальные call-центры под видом легальной организации. Объединение в подобные структуры позволяет им осуществлять масштабные и координированные операции, направленные на обман граждан и хищение их средств. Как правило, создание call-центра преступной группой включает в себя несколько этапов:

1) подбор «персонала» и его обучение: организаторы преступных группировки нанимают менеджеров, операторов, которые проходят обучение методикам обмана и психологическим приемам воздействия на потенциальных жертв. Иногда операторы часто не осведомлены о преступной природе предполагаемой деятельности или действуют осознанно, получая вознаграждение за участие в мошеннических схемах;

2) организация технического оснащения: для обеспечения бесперебойной работы call-центра приобретается необходимое оборудование и программное обеспечение, включая телефонные системы, программы

для управления звонками, сокрытия абонентских номеров;

3) разработка сценариев и алгоритмов совершения обманов: преступники разрабатывают подробные сценарии общения с потенциальными жертвами, включая легенды о непредвиденных обстоятельствах, требующих немедленного перевода средств, или предложения о получении крупных сумм денег за выполнение простых заданий. Вместе с тем участники обмана изучают информацию, необходимую для исполнения конкретной роли (например, кредитный специалист, сотрудник правоохранительных органов);

4) создание правил, регулирующих условия логистики, координации совместных действий, а также распределения доходов, добытых преступных путем: организуется логистическая поддержка и координация действий между операторами, менеджерами и другими участниками преступной схемы. Это обеспечивает эффективное взаимодействие и быстрое реагирование на изменения в ситуации.

Следы преступной деятельности. Материальные следы могут быть представлены в виде физических объектов, таких как устройства для доступа к сети, носители электронной информации, документы и другие предметы, которые использовались в ходе преступной деятельности. Основная часть криминалистически значимой информации о подобных преступлениях содержится в памяти различных компьютерных устройств, технологически предназначенных для использования файлов, сервисов, программ, имеющих функции, которые преступники адаптировали для разрешения преступных целей. К таким объектам следует отнести браузеры, программы, которые предназначены для обмена сообщениями, – мессенджеры, специальные приложения социальных сетей, онлайн-игр и др.

Справедливо отметить, что наибольшей значимостью обладают цифровые следы организованной преступной деятельности, которые представляют собой данные, зафиксированные в электронном виде на материальном носителе компьютерной информации, содержащие криминалистически значимые сведения о механизме совершения преступлений, свидетельствующие о связи соучастников в ходе подготовки и совершения данных преступлений. Так, при незаконном сбыте наркотических средств между участниками преступной группы обеспечивается связь с использованием электронных или информационно-телекоммуникационных сетей, включая сеть Интернет (между лицом, осуществляющим закладку наркотических средств в тайники, и лицом, передавшим ему в этих целях наркотические средства).

С учетом изложенного электронно-цифровые следы организованной преступной деятельности можно разделить на следующие виды:

– метаданные. Это сведения о данных, которые включают информацию о времени создания и изменения файлов, IP-адресах, геолокации и другой ценной информации о действиях преступников, их местоположении и связях;

– электронные сообщения и переписка. Сообщения, отправленные через электронные почтовые сервисы, мессенджеры, а также социальные сети, могут содержать важную информацию о планах, действиях и намерениях преступников. Анализ подобных сведений поможет выявить структуру группировки, роли участников и их связи;

– файлы и цифровые документы. Файлы, созданные и передаваемые в рамках преступной деятельности, могут содержать информацию о методах преступной деятельности группы, ее целях и задачах. К таким документам следует отнести чеки об операциях, фото и видеоматериалы, финансовые отчеты, инструкции и алгоритмы и т.д.;

– информация из журнала системных событий. Записи, создаваемые системами и приложениями в процессе работы с ними преступниками, могут включать информацию о входах в систему, обращениях к ресурсам, ошибках и других действиях. Анализ подобных записей может способствовать выявлению механизма совершения преступления, восстановлению хронологии действий преступников;

– сведения о финансовых транзакциях. Анализ подобной информации позволит опре-

делить источники финансирования преступной группы, правила распределения доходов, места обналичивания денежных средств и т.д.;

– информация о доступе к сетевым ресурсам. Записи о доступе к различным сетевым ресурсам (веб-сайтам, файловым серверам и т. п.) могут содержать информацию о том, какие ресурсы использовались преступниками, с каких IP-адресов осуществлялся доступ и т.д.;

– сведения, полученные в результате использования программного обеспечения для обеспечения анонимности. Несмотря на попытки преступников скрыть свою деятельность с помощью виртуальных частных сетей (VPN), прокси-серверов и других инструментов, все равно остаются электронно-цифровые следы, которые могут быть подвергнуты тщательному анализу и использованы для идентификации участников преступных групп.

К основным следам использования анонимайзеров можно отнести резкое изменение IP-адреса, особенно в тех случаях, когда IP-адрес внезапно меняется на такой адрес, который относится к другому географическому региону или известен как адрес анонимайзера. Вместе с тем существуют базы данных, содержащие IP-адреса, которые известны как адреса анонимайзеров. Обнаружение трафика, исходящего или входящего на такие адреса, может указывать на использование подобных технологий преступниками. Следами использования анонимайзеров могут быть сведения о нестандартных портах и протоколах, например, для Tor характерно использование порта 9050 или 9150 для своих узлов. Кроме того, признаками использования анонимайзеров также служит выявление информации о шифрование трафика. Это применяется преступниками для защиты передаваемых данных. Следовательно, наличие зашифрованного трафика, особенно если он идет через известные порты анонимайзеров, может быть еще одним следом их использования.

Таким образом, анализ типичных способов совершения преступлений, цифровых следов является важным инструментом в борьбе с организованной преступной деятельностью в цифровом пространстве. Анализ источников представленной информации позволит следователю идентифицировать участников преступной группировки, а также установить их местонахождение, восстановить хронологию событий и определить последовательность действий преступников, собрать доказательственную базу, изобличающих их вину, определить связи между соучастниками преступлений и др.

Библиографический список

1. Белкин, Р.С. Криминалистика : учебник / Р.С. Белкин. – М.: НОРМА, 2001. – 990 с.
2. Зуйков, Г.Г. Криминалистическое учение о способе совершения преступления : автореф. дис. … докт. юрид. наук / Г.Г. Зуйков. – М., 1970. – 30 с.
3. Каминский, А.М. Теоретические основы криминалистического анализа организованной преступной деятельности и возможности его практического использования : автореф. дис. … докт. юрид. наук / А.М. Каминский. – Нижний Новгород, 2008. – 53 с.
4. Колесниченко, А.Н. Общие положения методики расследования отдельных видов преступлений / А.Н. Колесниченко. – Харьков: Харьков. юрид. ин-т, 1965. – 28 с.
5. Комиссаров, В.И. Тактика допроса потерпевших от преступлений, совершаемых организованными группами лиц / В.И. Комиссаров, О.А. Лакаева. – М.: Юрлитинформ, 2004. – 158 с.
6. Куликов, В.И. Основы криминалистической теории организованной преступной деятельности / В.И. Куликов. – Ульяновск: Ульянов. обл. газ. изд-во, 1994. – 219 с.

7. Лозовский, Д.Н. Процессуальные, организационно-тактические и методические особенности расследования убийств, совершаемых организованной преступной группой : автореф. дис. … канд. юрид. наук. – Ростов-на-Дону, 2004. – 26 с.

8. Мазунин, Я.М. Проблемы теории и практики криминалистической методики расследования преступлений, совершаемых организованными преступными сообществами (преступными организациями) : дис. … докт. юрид. наук / Я.М. Мазунин. – Барнаул, 2005. – 504 с.

9. Осипенко, А.Л. Организованная преступность в сети Интернет / А.Л. Осипенко // Вестник Воронежского института МВД России. – 2012. – N 3. – С. 10-16.

10. Романов, А.И. Расследования уголовных дел об организации преступного сообщества (преступной организации) : учебное пособие / А.И. Романов. – М.: Спутник+, 2009. – 131 с.

11. Старостенко, Н.И. Особенности первоначального этапа расследования дистанционных хищений, совершенных с применением методов социальной инженерии / Н.И. Старостенко. – М.: Юрлитинформ, 2024. – 168 с.

12. Тишутина, И.В. Преодоление противодействия расследованию организованной преступной деятельности: организационные, правовые и тактические основы : автореф. дис. … докт. юрид. наук. – М., 2013. – 47 с.

13. Усманов, Р.А. Характеристика преступной деятельности, осуществляемой в сети Интернет посредством сервисов-анонимайзеров / Р.А. Усманов // Юридическая наука и правоохранительная практика. – 2018. – N 4(46). – С. 135-141.

14. Яблоков, Н.П. Организованная преступная деятельность: теория и практика расследования : учебное пособие / Н.П. Яблоков. – М.: НОРМА, 2023. – 224 с.

15. Яблоков, Н.П. Криминалистика : учебник / Н.П. Яблоков. – 2-е изд., перераб. и доп. – М.: Норма, 2008. – 784 с.