УДК 343.57

М. Г. Ермаков
Омская академия МВД России

Выявление и раскрытие сбыта подконтрольных веществ, совершенного дистанционным способом с использованием сети Интернет

АННОТАЦИЯ. *Введение.* Интернет является популярной площадкой для обмена информацией в целях приобретения или сбыта различного вида подконтрольных веществ. Обращение к международному опыту свидетельствует, что эта проблема характерна не только для России, но и для многих стран международного сообщества.

Результаты и выводы. Рассматриваются современные способы распространения наркотических средств с использованием сети Интернет, предлагается алгоритм действий сотрудников оперативных подразделений по поиску необходимой информации о функционировании преступных групп путем проведения соответствующих оперативно-розыскных мероприятий и меры по противодействию им, а также высказываются рекомендации по повышению эффективности работы в данном направлении.

КЛЮЧЕВЫЕ СЛОВА: наркотические средства, сбыт наркотиков, дистанционный способ, сеть Интернет, алгоритм действий.

ДЛЯ ЦИТИРОВАНИЯ: Ермаков М. Г. Выявление и раскрытие сбыта подконтрольных веществ, совершенного дистанционным способом с использованием сети Интернет // Научный портал МВД России. 2020. № 3 (51). С. 66–72.

M. G. Ermakov
Omsk Academy of the Ministry of the Interior of the Russian Federation

Identification and disclosure of the sale of controlled substances carried out remotely using the internet

ABSTRACT. *Introduction.* Currently, the Internet is a popular platform for the exchange of information for the purchase or sale of various types of controlled substances. The appeal to international experience shows that this problem is typical not only for Russia, but also for many countries of the international community.

Results and Conclusions. The article deals with modern methods of distribution of narcotic drugs using the Internet, offers an algorithm of action of employees of operational units to find the necessary information about the functioning of criminal groups by carrying out appropriate operational and investigative measures and measures to counteract, as well as makes recommendations to improve the efficiency of work in this area.

KEYWORDS: drugs, drug sales, remote method, Internet, algorithm of actions.

FOR CITATION: Ermakov M. G. Identification and disclosure of the sale of controlled substances carried out remotely using the internet // Scientific portal of the Russia Ministry of the Interior. 2020. № 3 (51). P. 66–72 (in Russ.).

Современные средства и способы доставки и оплаты товаров порождают новые способы распространения подконтрольных веществ, которыми пользуются как организованные группы (далее – ОГ), так и отдельные преступные элементы по всему миру. Речь идет прежде всего о возможностях, предоставляемых сетью Интернет. Одним из первых официальных международных документов, указавших на данную проблему, стал доклад Международного комитета по контролю над наркотиками ООН (далее – МККН) за 1998 г., где отмечалось, что «использование таких новых технологий, как система „World Wide Web", представляет все более значительную угрозу для международных и национальных мер контроля. Наркотики и соответству-

ющие принадлежности открыто продаются через Web-узлы»[1].

Через 13 лет в докладе за 2011 г. МККН уделил данной проблеме особое внимание. Доклад во многом был посвящен проблемам борьбы с незаконным сбытом психоактивных веществ с использованием сети Интернет. В нем говорится, что «в течение последних нескольких лет Комитет неоднократно обращал внимание правительств на необходимость проведения совместной работы по расследованию и пресечению деятельности незаконных интернет-аптек и изъятию веществ, незаконно заказываемых через Интернет и доставляемых по почте»[2]. Комитет отмечает, что «торговля веществами, находящимися под международным контролем, через незаконные интернет-аптеки продолжает процветать, а сами аптеки пользуются все более разнообразными средствами для осуществления своей деятельности. После того как несколько поисковых интернет-серверов запретили использовать в рекламных ссылках зарегистрированные товарные знаки лекарственных препаратов, отпускаемых по рецепту врача, незаконные интернет-аптеки стали все активнее рекламировать свои веб-сайты через интернет-форумы и социальные сети»[3].

Учитывая рекомендации Комитета, в ст. 228.1 УК РФ были внесены изменения[4] и с 1 января 2013 г. установлена ответственность за сбыт наркотических средств, психотропных веществ или их аналогов с использованием средств массовой информации либо электронных или информационно-телекоммуникационных сетей (включая сеть Интернет) как квалифицированный состав незаконного сбыта, однако данное нововведение до сих пор не повлияло на оценку аналогичных действий с сильнодействующими и ядовитыми веществами.

В докладе МККН за 2016 г. указано, что «многие из новых психоактивных веществ, обнаруженных в Европе, были изготовлены компаниями, действующими на законных основаниях в Китае и, реже, в Индии. Эти компании через свои веб-сайты и интернет-магазины извещают о наличии у них возможностей для поставки новых психоактивных веществ в количествах от нескольких миллиграммов до сотен килограммов. Из стран-изготовителей крупные партии таких веществ отправляются в Европу морским или воздушным путем; меньшие количества доставляются покупателям напрямую экспресс-почтой и курьерскими службами»[5].

В опубликованном докладе МККН за 2017 г. отмечается, что «незаконные интернет-аптеки становятся все более массовым явлением, которое может вызвать серьезные проблемы в области здравоохранения. Продолжающийся рост доступа к Интернету во всем мире, широкая доступность онлайновых каналов связи и масштабы „глубокой сети" содействуют тому, что незаконный оборот наркотиков через Интернет, будь то через незаконные интернет-аптеки или другими средствами, становится значительной угрозой правопорядку»[6].

Данные по России в докладе отсутствуют, однако проведенное нами исследование подтверждает отмеченную общую тенденцию к распространению подконтрольных веществ с использованием сети Интернет.

Как отмечают исследователи, повышенная общественная опасность использования сети Интернет при совершении преступлений заключается в том, что «сама природа сети Интернет зачастую является благоприятной для совершения преступлений, так как такие ее свойства, как глобальность, трансграничность, анонимность пользователей, охват широкой аудитории, распределение основных узлов сети и их взаимозаменяемость, создают преступникам, использующим Интернет, преимущества на всех этапах совершения преступления, а также позволяют эффективно скрываться от правоохранительных органов» [1, с. 7].

Изучение материалов уголовных дел, расследованных территориальными органами внутренних дел Российской Федерации, позволяет сделать вывод о том, что существует множество схем сбыта подконтрольных веществ с помощью сети Интернет. Каждая схема индивидуальна, строится организаторами преступных групп исходя из их личных навыков и возможностей, а также с учетом особенностей менталитета жителей конкретного региона.

---

[1] См.: Доклад Международного комитета по контролю над наркотиками ООН за 1998 г. Нью-Йорк, 1999 (извлечения) // Бабаян Э. А., Бардин Е. В., Гаевский А. В. Правовые аспекты оборота наркотических, психотропных, сильнодействующих, ядовитых веществ и прекурсоров. Государственные и ведомственные акты. Методические материалы. Комментарии. Ответы на вопросы : в 2 ч. М., 2002. Ч. 2. С. 102.

[2] Доклад Международного комитета по контролю над наркотиками ООН за 2011 г. Нью-Йорк, 2012. С. 48.

[3] Там же. С. 49–50.

[4] См.: О внесении изменений в отдельные законодательные акты Российской Федерации : Федер. закон от 1 марта 2012 г. № 18-ФЗ // Рос. газ. 2012. 6 марта.

[5] Доклад Международного комитета по контролю над наркотиками ООН за 2016 г. Нью-Йорк, 2017. С. 103.

[6] Доклад Международного комитета по контролю над наркотиками ООН за 2017 г. Вена, 2018. С. 126.

В особо крупных организованных преступных группах (далее – ОПГ) могут дополнительно появляться должности «кураторов» по направлениям деятельности: по территориальному принципу курирования сегментов ОПГ, действующих на определенной территории (город, регион и т. п.), по принципу сферы деятельности – курирование деятельности определенных уровней ОПГ (операторы, закладчики т. п.). Чем меньше объемы оборота группы, тем меньшее количество лиц втянуто в деятельность группы. Соответственно в таких случаях некоторые функции выполняются одним человеком вплоть до того, что организатор, оператор и закладчик могут быть одним лицом. Чаще всего при работе магазина в пределах одного населенного пункта организатор берет на себя обязанности оператора.

Типовая схема сбыта подконтрольных веществ включает следующие стадии:

1. Размещение информации о продаже наркотических средств или иных подконтрольных веществ на специализированных сайтах, форумах, в социальных сетях, на сайтах знакомств и бесплатных досках объявлений, где в качестве контактных данных указывают никнейм (сетевое имя – псевдоним) в интернет-сервисах «Skype», «Brosix», «ooVoo», «Jabber», «Whatsapp», «Viber», «Telegram» и др. В некоторых случаях может быть указан номер интернет-мессенджера, адрес почтового ящика либо номер сотового телефона. В социальных сетях («ВКонтакте», «Одноклассники», «Mail.ru» и др.) и на досках объявлений, как правило, размещаются предложения о приобретении сильнодействующих веществ (биологически активных добавок для похудения, анаболических стероидов), так как в целях предотвращения блокирования указанных ресурсов размещаемая информация подлежит модерации, а информация о сильнодействующих веществах не вызывает опасений у администрации данных сайтов. Кроме этого, часто встречается реклама в виде «граффити», нанесенная на заборах, гаражах, домах и т. п., с указанием контактных данных.

2. Связь приобретателя со сбытчиком путем личной переписки. Как правило, у сбытчика наркотиков имеется заранее готовый прайс предлагаемых веществ с указанием цены и веса. Также в ходе переписки потребителю сообщается информация о способах оплаты и получения приобретаемого вещества.

3. Оплата заказа в большинстве случаев осуществляется безналичным расчетом путем перевода денежных средств на электронный счет платежных систем «Visa Qiwi Wallet», «WebMoney», «Яндекс-деньги». В последнее время отмечено использование платежной системы «BitCoin».

4. Проверка поступления денежных средств и осуществление закладок наркотиков в тайник («закладку») либо предоставление заранее готовых адресов тайников.

5. Сообщение приобретателю описания места закладки наркотиков посредством указанных программных клиентов интернет-связи.

Наиболее эффективным способом выявления данных преступлений является организация многоступенчатой системы получения информации, включающая:

1) обращения и заявления граждан о совершаемых преступлениях, поступающие в территориальные органы внутренних дел;

2) информацию, непосредственно получаемую оперативным сотрудником, в том числе из сети Интернет, путем проведенного поиска с использованием специализированных сайтов (форумов) либо поисковых сайтов («Yandex», «Google» и др.);

3) информацию, получаемую из других территориальных органов.

Примерный общий алгоритм проведения оперативно-розыскных мероприятий выглядит следующим образом.

В сети Интернет с использованием поисковых систем («Yandex», «Google» и др.) обнаруживается информация о продаже подконтрольных веществ и выявляются контактные данные участвующих в этом лиц. Указанная информация в основном содержится на специально зарегистрированных для этих целей сайтах и форумах, а также на бесплатных досках объявлений, в социальных сетях и т. п.

Следует отметить, что результаты поиска необходимо рассматривать как сведения, подлежащие дальнейшей тщательной проверке. Это обусловлено тем, что авторами объявлений и иной информации могут быть лица, целью которых является завладение денежными средствами приобретателей мошенническим путем. Учитывая данный факт, результативность поиска напрямую зависит от имеющихся сведений, с использованием которых строится поисковый запрос. Наиболее эффективным является поиск информации на специализированных ресурсах, пользующихся доверием со стороны потребителей.

Основными источниками наиболее достоверной информации, используемыми при поиске в сети Интернет, являются:

сведения, получаемые от ранее задержанных лиц (названия магазинов, контактные данные

сбытчика, интернет-ресурсы, где были обнаружены контактные данные сбытчика);

сведения, получаемые в ходе оперативно-розыскных мероприятий.

Таким образом, в результате проведения оперативного поиска сотрудник получает определенный массив информации, размещенной в сети Интернет на специализированных форумах, в социальных сетях, на досках объявлений и т. п., требующий определенной проверки.

На следующем этапе путем переписки (как правило, через интернет-мессенджеры) устанавливается контакт с лицом, разместившим объявление. На данном этапе оперативный сотрудник обычно контактирует с «оператором». Следует отметить, что в ходе общения «оператор» почти всегда соблюдает конспирацию и выдает незначительную часть информации, поэтому важно добиться доверия с его стороны. В ходе общения выявляется информация о виде и размере сбываемого наркотика (торговое или химическое название), действии, оказываемом на организм, фасовке, упаковке, цене, возможном способе приобретения (посредством почтовых отправлений, путем доставки курьерской службой, с нарочным, тайниковым способом и т. п.).

Дальнейшие оперативно-розыскные мероприятия можно разбить на два этапа. Первый этап – установление лиц, причастных к деятельности магазина. Второй этап – документирование их преступной деятельности.

Первоначальные оперативно-розыскные мероприятия целесообразно проводить по следующим направлениям.

1. Получение данных об «операторе».

2. Получение данных о переводах денежных средств.

Работа по первому направлению включает решение узкого круга задач:

установление местонахождения «оператора»;

определение регистрации «оператора» у конкретного интернет-провайдера;

установление физического лица, являющегося «оператором».

В дальнейшем, отрабатывая контакты «оператора» с иными лицами, возможно установить «закладчика» и иных членов группы. Ключевым моментом данного этапа является получение персональных данных лица, причастного к сбыту наркотиков, посредством выявленных контактных данных (никнейм в интернет-программе обмена информацией и т. п.) и выявление IP-адреса – идентификатора интернет-соединения. Определение привязки IP-адреса к конкретному физическому лицу является важнейшим моментом на данном этапе и, как правило, обусловливает возможность и целесообразность проведения дальнейших оперативно-розыскных мероприятий (далее – ОРМ) в отношении фигурантов.

Определение IP-адреса, как правило, осуществляется посредством привлечения специалистов в области информационных систем и технологий, в качестве которых могут выступать должностные лица специализированных подразделений органов, осуществляющих оперативно-розыскную деятельность, либо иные граждане, обладающие специальными познаниями в данной области.

Зачастую наркосбытчик скрывает свой реальный IP-адрес при помощи специальных программных инструментов по его сокрытию (использование анонимайзеров, TOR, VPN-сервисов[7] и прокси-серверов). Данные инструменты в сети Интернет позволяют скрывать сведения об источнике запроса или пользователе. В таком случае при установлении IP-адреса оперативный сотрудник видит лишь информацию о прокси-сервере (в основном это IP-адреса устройств, находящихся за рубежом, например в Испании, Египте, Китае, которые могут меняться через короткий промежуток времени), но не имеет возможности определить истинный источник запроса.

Также в случае использования наркосбытчиком GSM-соединения для выхода в сеть Интернет (3G, 4G usb-модемы) оперативному сотруднику не удается установить местонахождение и персональные данные лица. Это связано с тем, что при работе с Интернетом операторы сотовой связи присваивают один и тот же динамический IP-адрес нескольким подключенным устройствам одновременно и не имеют специального оборудования, которое бы хранило информацию о присвоении динамическим IP-адресам идентификационных данных устройства[8]. Если бы у операторов сотовой связи были такие возможности, то при направлении запроса с указанием определенного IP-адреса наркосбытчика и точного вре-

[7] VPN (англ. «Virtual Private Network» – виртуальная частная сеть) – обобщенное название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети (например, Интернет), в том числе с использованием средств криптографии.

[8] Динамический IP-адрес уникален только в ограниченный промежуток времени. Идентификатором устройств, использующих мобильные сети для выхода в сеть Интернет, является IMEI, для стационарных устройств – MAC. В связи с этим имеет смысл направлять провайдерам запросы о принадлежности выявленного IMEI и MAC-адреса (номера симкарт в мобильных устройствах, на кого оформлены договоры, какой физический адрес канала и т. д.).

мени входа в сеть Интернет можно было бы установить идентификационные данные устройства, например IMEI сотового телефона, что позволило бы установить номер SIM-карты и ее владельца.

Если оперативному сотруднику удалось установить статический IP-адрес, то дальнейший алгоритм работы будет построен следующим образом.

По установленному IP-адресу с помощью программного интерфейса «Whois» определяется географическое местоположение узла компьютерной сети абонента, а также провайдер, в диапазон которого входит интересующий IP-адрес. Кроме того, возможно использовать другие ресурсы, например на сайте www.2ip.ru, предоставляющем дополнительные инструменты.

После установления провайдера проводится ОРМ «Наведение справок». Для этого в адрес провайдера направляется запрос о предоставлении сведений о присвоении IP-адреса своему клиенту. Ответ содержит сведения (ФИО, адрес подключения, контактный телефон и иное) о физическом или юридическом лице, которому был выдан IP-адрес на основании договора оказания услуг. Посредством запроса в организацию-провайдер устанавливаются персональные данные лица, на которое зарегистрирован интересующий IP-адрес. Необходимо отметить, что все чаще встречаются факты использования ресурсов, зарегистрированных в доменной зоне COM, NET, BIZ и т. п., находящихся на хостинге за пределами Российской Федерации. В этом случае получение дополнительной информации затруднительно. В случае расположения хостинга в странах ЕС или Северной Америке необходимо рассматривать возможность направления запросов на получение интересующей информации в правоохранительные органы соответствующей страны по линии международного сотрудничества МВД России.

Полученные сведения о персональных данных лица используются для проведения комплекса ОРМ.

Основной задачей работы по второму направлению является установление электронных счетов платежных систем, на которые переводятся денежные средства за оплату подконтрольных веществ. В зависимости от вида платежной системы, в которой открыт электронный счет («Visa Qiwi Wallet», «WebMoney», «Яндекс-деньги» и др.), осуществляется мероприятие по получению сведений о движении денежных средств посредством официального запроса в соответствующую компанию для получения следующих сведений: персональные данные лица, прошедшего идентификацию, привязанные к счету банковские карты, приходные и расходные операции по счету за весь период срока действия с указанием реквизитов платежей, IP-адресов, MAC-адресов, времени выхода в систему, используемых терминалов и другая оперативно значимая информация.

Так, например, ответ из «Qiwi» содержит следующую информацию:

дата регистрации кошелька, а также IP-адрес, использованный при данной операции;

дата и время совершения операций по счету;

источники получения денежных средств;

IP-адрес лица, проводящего операции.

Аналогичными сведениями обладают и другие используемые платежные системы, в том числе банки, предоставляющие услуги удаленного управления счетом.

Также в ответах операторов платежных систем содержатся сведения о движении денежных средств, направленных на их вывод в наличную форму. Как правило, это номера счетов банковских карт, куда выводят денежные средства. При получении подобной информации оперативному сотруднику необходимо получать в соответствующих банковских организациях сведения о владельцах счетов и способах обналичивания денежных средств.

Однако следует учитывать, что заявленные регистрационные данные не всегда содержат достоверную информацию, последнее зависит от процедуры проверки данных администрацией платежной системы. Сведения о проведении операций с электронными денежными средствами (транзакций) не относятся к сведениям, составляющим банковскую тайну. Вместе с тем переводы денежных средств, осуществляемые с использованием компаний, специализирующихся на предоставлении услуг денежного посредничества («Western Union», «Контакт», «Связной» и др.), и переводы на счета организаций относятся к сведениям, составляющим банковскую тайну, и представляются на основании запросов следственных органов по уголовному делу или по решению суда. Однако получаемая информация содержит подтвержденные сведения об отправителе и получателе перевода.

Анализ исходящих платежей с электронного счета позволяет установить начальную цепочку «отмывания» денежных средств. В случае использования для вывода денежных средств банковских счетов и карт в соответствии с положениями Федерального закона от 2 декабря 1990 г. № 395-1 «О банках и банковской деятельности» направляется запрос в кредитно-финансовую орга-

низацию на получение выписки по счетам. Впоследствии при ее получении проводится судебная экономическая экспертиза для полного анализа схемы «отмывания» денежных средств. Из практики следует, что наркосбытчики для обналичивания денежных средств приобретают аналогичным бесконтактным способом в сети Интернет так называемые анонимные банковские карты и SIM-карты, что не позволяет установить персональные данные лица. В таком случае по выписке со счета банковской карты можно установить информацию об используемых для обналичивания денежных средств банкоматах, а также о пунктах сферы обслуживания, в которых посредством карты осуществлялась оплата за товары, услуги и т. д. Анализ информации позволит на карте населенного пункта обозначить места появления владельца банковской карты и частоту операций по карте. Для получения изображения лица запрашиваются видеозаписи, на которых владелец карты или иное лицо по его поручению производит обналичивание денежных средств в банкомате или использует данную карту в иных местах, где осуществляется видеозапись (заправки, гостиницы и т. п.). Также ценной является информация о подключенных дополнительных услугах пользователем счета, функционирование которых зачастую осуществляется с использованием номера сотового телефона или сервиса «bank online» (запрос баланса, подтверждение операции по счету), что позволяет проводить дальнейшие мероприятия по установлению лица.

Также из анализа движений денежных средств по используемым счетам можно установить:

счета, на которых аккумулируется основная часть денежной массы. Эти счета находятся в пользовании организаторов сбыта, и целенаправленное проведение комплекса ОРМ по ним дает возможность установления их личностей;

счета, на которые выводятся до 15 % от общей суммы денег, поступающих на счет магазина на протяжении длительного времени с определенной периодичностью. Данные операции чаще всего являются выплатой заработной платы участникам сбыта;

счета, на которые выводятся значительные суммы за короткий промежуток времени. Это, как правило, счета поставщиков сбываемых веществ.

Установление персональных данных лица (ОРМ «Наведение справок») путем направления запросов в соответствующие органы осуществляется одновременно с мониторингом социальных сетей («ВКонтакте», «Одноклассники» и др.) для получения дополнительных сведений о лице (месте работы, учебы, досуга, увлечении, наличии транспорта и т. д.), а также выявления его связей и сохранения фотографий.

Чтобы проверить, какое именно вещество сбывается, необходимо получить образцы данных веществ. Результат исследования образцов позволит определить название вещества и соответственно установить, является ли оно подконтрольным. С указанной целью возможно проведение ОРМ:

оперативного эксперимента – для установления механизма действия сбытчиков и получения данных о них;

проверочной закупки – при наличии данных о лицах, сбывающих подконтрольные вещества.

В некоторых случаях новые магазины на этапе выхода на рынок сбыта психоактивных веществ с целью получения положительных отзывов среди потребителей активно раздают некоторое количество «пробников», которые можно получить безвозмездно. Кроме того, при определенной изобретательности, например сославшись на боязнь мошенников либо высказав намерения о приобретении оптовых партий, возможно получение безвозмездного пробника и от магазина, уже прошедшего этап становления.

Далее, организуя и проводя ОРМ, осуществляется документирование противоправной деятельности фигурантов дела, определяются роль и место каждого, создаются условия для прекращения их преступной деятельности. Однако в ряде случаев, чтобы доказать вину фигурантов, необходимо проведение ряда следственных действий, которые возможны только в рамках возбужденного уголовного дела. Поэтому целесообразно задержание «низовых» участников групп и планирование комплекса оперативно-следственных мероприятий.

Таким образом, результативность установления конкретных лиц, совершающих преступления с использованием сети Интернет, а также документирования данных преступлений напрямую зависит от творческих способностей оперативного сотрудника и его знаний в области сетевых технологий. В качестве рекомендаций для более эффективного противодействия данному способу совершения преступлений и в целях успешного выявления и пресечения деятельности указанных преступных групп в территориальных органах внутренних дел целесообразно:

организовать подготовку сотрудников, которые будут заниматься выявлением преступлений на данном направлении, обеспечив им свобод-

ный доступ к сети Интернет с использованием средств анонимизации IP-адреса;

организовать систему получения оперативной информации в указанной сфере (в том числе мониторинг сайтов и рекламы продаж псевдолегальных наркотиков, интернет-магазинов по продаже товаров наркотической тематики и др.).

Рассмотренная схема и способы сбыта подконтрольных веществ являются достаточно «молодыми», в связи с чем методика выявления и расследования также нова и продолжает совершенствоваться. В то же время между лицами, совершающими преступления в данной сфере, происходит постоянный обмен опытом и информацией и, как следствие, ими вырабатываются новые способы ведения «бизнеса». К примеру, последнее время ими предпринимаются попытки перехода на использование в денежных расчетах криптовалют и новых систем обмена сообщениями, обеспечивающих большую безопасность и анонимность. С учетом этих тенденций составить полные, исчерпывающие рекомендации по противодействию преступлениям указанной категории просто не представляется возможным, однако изложенный материал может служить отправной точкой в наработке собственного уникального опыта.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Дремлюга Р. И. Интернет-преступность : автореф. дис. … канд. юрид. наук. – Владивосток, 2007. – 25 с.

REFERENCES

1. Dremlyuga R. I. *Internet-prestupnost' : avtoref. dis. … kand. yurid. nauk* (Internet Crime: Extended abstract of candidate's thesis), Vladivostok, 2007, 25 p.

Рукопись поступила в редакцию 15.01.2020, принята к публикации 14.09.2020.

ИНФОРМАЦИЯ ОБ АВТОРЕ

Михаил Геннадьевич Ермаков, кандидат юридических наук, старший преподаватель кафедры криминалистики федерального государственного казенного образовательного учреждения высшего образования «Омская академия Министерства внутренних дел Российской Федерации» (Российская Федерация, 644092, г. Омск, пр. Комарова, д. 7)

E-mail: mgermakov@yandex.ru

Тел.: 8 (3812) 75-11-13 (доб. 2-31)

INFORMATION ABOUT THE AUTHOR

Mikhail G. Ermakov, Candidate of Juridical Sciences, Senior lecturer of the chair of criminalistics, Federal State Educational Institution of Higher Education Omsk Academy of the Ministry of Internal Affairs of the Russian Federation (Omsk, Komarova ave., 7, 644092, Russian Federation)

E-mail: mgermakov@yandex.ru

Tel.: 8 (3812) 75-11-13 (ext. 2-31)