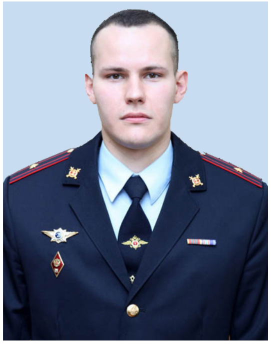
Научная статья
УДК 341:31
https://doi.org/10.36511/2078-5356-2024-2-73-79



Содержание оперативно-розыскного мероприятия «Наведение справок» при выявлении и раскрытии преступлений, совершаемых с использованием сети «Интернет»

Захаров Николай Дмитриевич
Волгоградская академия МВД России, Волгоград, Россия, ratinho@bk.ru

Аннотация. В статье рассматриваются различные способы, формы, методы и ожидаемые результаты проведения оперативно-розыскных мероприятий «Наведение справок» в зависимости от складывающейся обстановки при выявлении и раскрытии преступлений, совершаемых с использованием сети «Интернет» с учетом возможностей, представляемых информационно-телекоммуникационными сетями на современном этапе. На основе правовых, организационных, тактических и технических особенностей рассматриваются различные направления проведения ОРМ «Наведение справок» как непосредственно в сети «Интернет», так и возможности применения информационно-поисковых систем, стоящих на обеспечении полиции, а также находящихся в свободном доступе.

Ключевые слова: оперативно-розыскная деятельность, оперативно-розыскные мероприятия, наведение справок, интернет, информационные системы

Для цитирования: Захаров Н. Д. Содержание оперативно-розыскного мероприятия «Наведение справок» при выявлении и раскрытии преступлений, совершаемых с использованием сети «Интернет» // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2024. № 2 (66). С. 73–79. https://doi.org/10.36511/2078-5356-2024-2-73-79.

Original article

The main directions of the operational search activity “Making inquiries” in the identification and disclosure of crimes committed using the Internet

Nikolai D. Zakharov
Volgograd Academy of the Ministry of Internal Affairs of Russia, Volgograd, Russian Federation, ratinho@bk.ru

Abstract. The article discusses various methods, forms, methods and expected results of conducting an operational search event “Making inquiries”, depending on the current situation in identifying and solving crimes committed using the Internet, taking into account the possibilities presented by information and telecommunications networks at the present stage. On the basis of legal, organizational, tactical and technical features, various directions of conducting the ORM “Making inquiries” are considered both directly on the Internet, and the possibility of using information search engines that support the police, as well as those that are freely available.

***Keywords**:* operational investigative activities, operational investigative measures, inquiries, Internet, information systems

For citation: Zakharov N. D. The main directions of the operational search activity “Making inquiries” in the identification and disclosure of crimes committed using the Internet. *Legal science and practice: Journal of the Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia*, 2024, no. 2 (66), pp. 73–79 (In Russ.). https://doi.org/10.36511/2078-5356-2024-2-73-79.

Развитие информационно-телекоммуникационных технологий предопределило рост числа преступлений, совершаемых в рассматриваемой сфере. Реагируя как на современные внутренние вызовы в государстве, так и резко осложнившуюся внешнеполитическую обстановку, МВД России во взаимодействии с иными государственными, в том числе не правоохранительными органами, организует работу, направленную на противодействие преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий.

Особую значимость здесь приобретает использование сил, средств и методов оперативно-розыскной деятельности (далее — ОРД) как одного из действенных элементов системы обеспечения национальной безопасности Российской Федерации.

На сегодняшний день остается дискуссионным вопрос о правовой регламентации проведения оперативно-розыскных мероприятий (далее — ОРМ) в сети «Интернет». Не ставя в настоящем исследовании задачу уяснить теоретико-правовые основы осуществления ОРД в сети «Интернет», отметим, что анализ научной литературы и нормативной правовой базы позволил нам полностью разделить позицию известного ученого в рассматриваемой сфере доктора юридических наук, профессора В. И. Шарова, высказанную еще в 2018 году, но не потерявшую актуальность и сегодня, указывающего, что единая концепция по получению и использованию информации из сети «Интернет» в процессе ОРД не сформирована окончательно, алгоритм действий в принципе понятен, но законность и целесообразность таких действий во многих случаях требуют объяснения [1, с. 82].

Представляется, что по причине отсутствия закрепленных на государственном уровне правовых основ деятельности субъектов ОРД в сети «Интернет» разрешение данной проблемы лежит в плоскости определения различных форм, средств и методов проведения ОРМ в сети «Интернет» и их документального оформления.

Таким образом, в настоящей статье мы умышленно не затрагивали дискуссионные вопросы, связанные с пониманием содержания и пределов проводимых в сети «Интернет» ОРМ, и сфокусировали усилия на рассмотрении конкретных способов проведения ОРМ «Наведение справок» в сети «Интернет» как одного из самых перспективных, по нашему мнению, мероприятий, представляющих оперативному сотруднику богатый функционал как с точки зрения правовых основ и универсальности в выборе форм, средств и методов проведения, так и широкого пласта информации, получаемой по его результатам.

Изучение архивных уголовных дел, анализ научной литературы и результатов интервьюирования респондентов — сотрудников оперативных подразделений ОВД, а также личный практический опыт автора [2] позволили выделить следующие основные направления проведения ОРМ «Наведение справок».

1. Установление технической информации (регистрационных данных) о пользователе, создавшем и администрирующем страницу в социальной сети [3, с. 112]. Каждый зарегистрированный пользователь социальной сети, как и каждая созданная в ней группа (сообщество), имеют персональный идентификационный номер так называемый *ID*. При получении информации в отношении конкретного аккаунта (сообщества) оперативному сотруднику необходимо направить соответствующий запрос в адрес администрации ресурса. В зависимости от задач, стоящих перед оперативным сотрудником, могут быть получены следующие сведения:

— адрес и наименование страницы, указанные при регистрации анкетные данные;

— дата, время и *IP*-адрес регистрации страницы;

— номер телефона, привязанный к аккаунту (для *SMS*-подтверждения при прохождении двухфакторной аутентификации);

— электронная почта, привязанная к аккаунту;

— время последнего изменения пароля и *IP*-адрес, с которого было совершено это действие;

— история изменений имени пользователя и привязки телефонного номера;

— время размещения указанного в запросе контента и *IP*-адрес, с которого он был опубликован;

— список *IP*-адресов, с которых осуществлялся вход на страницу;

— история блокировок страницы и обращений в техподдержку;

— сведения о произведенных в социальной сети платежных операциях;

— информация о списке друзей пользователя;

— операционная система и браузер, использующиеся на устройстве пользователя [4, с. 114].

Аналогичные данные могут быть получены и в отношении группы (сообщества): имена ее создателей и членов, время и *IP*-адрес, с которого осуществлялась публикация сообщения в группе.

2. Установление владельцев сайтов, ресурсов, доменных имен (включая способы оплаты за эти услуги) [3, с. 112]. Для установления лица, создавшего сайт, возможно использовать бесплатные и общедоступные интернет-сервисы типа *Whois* (например, *2ip.ru/whois/*, *reg.ru/whois/* и др.). В первую очередь следует определить компанию — регистратора доменного имени ресурса и компанию, на технических площадках которой размещен ресурс (хостинг-провайдера). После этого в адрес компании направляется запрос о предоставлении сведений, с каких *IP*-адресов создавался и администрировался сайт, о способах оплаты услуг, а также информации, указанной о себе лицом при регистрации данного сайта.

Указанные регистрационные данные не подлежат обязательной проверке (идентификации личности) со стороны регистратора доменного имени и (или) хостинг-провайдера и могут умышленно искажаться злоумышленниками. Но указанные сведения все равно целесообразно запрашивать и проверять, так как в ответе компании могут содержаться и *IP*-адреса авторизации, платежные реквизиты, адрес электронного почтового ящика создателя ресурса.

3. Установление сведений по электронному почтовому ящику (далее — ЭПЯ) и облачным хранилищам данных [3, с. 112]. Для установления владельца ЭПЯ необходимо направить соответствующий запрос в адрес владельца почтового клиента (например, *@mail.ru, @yandex.ru, @ramler.ru* и др.). Отметим, что такие организации могут быть зарегистрированы и за рубежом *(@gmail.com, @hotmail.com, @yahoo.com*).

В данном контексте необходимо отметить, что и операторы связи, и организаторы распространения информации в сети «Интернет» обязаны предоставлять информацию уполномоченным государственным органам, осуществляющим ОРД или обеспечение безопасности Российской Федерации, в случаях, установленных федеральными законами.

Необходимую информацию уполномоченные органы могут получить не только от российских организаций — собственников интернет-сервисов, но и от организаций, зарегистрированных вне юрисдикции Российской Федерации, но осуществляющих свою деятельность на ее территории [5]. Речь идет о так называемом законе о «приземлении» [6].

Указанный закон определил обязанность владельцев иностранных информационных ресурсов с суточной аудиторией более полумиллиона российских пользователей организовать в Российской Федерации свое представительство (учредить юридическое лицо), зарегистрировать личный кабинет на сайте Роскомнадзора, а также разместить на своем ресурсе электронную форму для обратной связи с российскими гражданами или организациями. Ранее законодательство не налагало указанных обязанностей на иностранные организации, что формально позволяло уклоняться от ответа на поступающие запросы правоохранительных органов.

Возвращаясь к результатам рассматриваемого способа проведения ОРМ, отметим, что могут быть получены следующие сведения:

— указанные при регистрации анкетные данные;

— дата, время и *IP*-адрес регистрации ЭПЯ;

— номер телефона, привязанный к ЭПЯ;

— дополнительная электронная почта, привязанная к аккаунту;

— сведения о произведенных платежных операциях;

— список *IP*-адресов, с которых осуществлялся вход на ЭПЯ;

— история изменений ЭПЯ, смены номера телефона, других данных.

Аналогичного алгоритма следует придерживаться и при установлении лица, создавшего облачное хранилище данных (как правило, на базе существующего аккаунта почтового клиента) — модель онлайн-хранилища, где данные хранятся на многочисленных распределенных в сети серверах, предоставляемых в пользование клиентам, — в так называемом «облаке», которое, с точки зрения клиента, является одним большим виртуальным сервером.

4. Установление сведений о владельцах электронного кошелька (электронной платежной системы) [3, с. 112]. Наиболее распространенными сервисами перевода электронных денежных средств в настоящее время являются *ЮMoney*, *YandexMoney*, *PayPal* и др. Следует учитывать, что функциональные возможности данных систем определены федеральным законом [7] и зависят от прохождения пользователем процедуры идентификации, которая позволяет осуществлять платежи и переводы без ограничений, а также расширяет возможности по снятию денежных средств. В случае ее прохождения пользователь сообщает исчерпывающие сведения о своей личности. Если этого не произошло, то его финансовая активность ограничивается. Однако стоит учитывать возможность использования злоумышленниками поддельных документов, удостоверяющих личность, либо задействования в этих целях подставных лиц. В названных организациях возможно запросить сведения о сеансах доступа к учетной записи (перечень технической информации соответствует рассмотренным выше примерам). При необходимости получения выписки о движении денежных средств по счетам требуется судебное решение, которое направляется в организацию. В ответе могут содержаться персональные данные, реквизиты банковских карт или номера электронных кошельков, связанные со счетом (пополнение баланса, переводы по номеру телефона), об абонентских номерах телефонов, о детализации финансовых операций.

5. Установление принадлежности IP-адреса. При получении от соответствующей организации сведений о дате, времени и конкретном *IP*-адресе обращения к ресурсу важнейшим этапом документирования является установление адреса конечного оборудования, а также личности конкретного лица, осуществляющего выход в сеть «Интернет».

Для определения провайдера используются общедоступные интернет-сервисы *Whois.* При установлении соответствующей организации в ее адрес направляется запрос, где указываются искомый *IP*-адрес, точные дата и время обращения к ресурсу, при наличии сведения о ресурсе, к которому осуществлялось обращение, что может значительно сузить рамки поиска интересующей информации. В ответе на запрос возможно получить следующие сведения:

— наименование логина, присвоенного пользователю;

— номер, дату заключения договора об оказании услуг связи;

— адрес оказания услуг;

— анкетные данные и контактный телефон абонента;

— способы оплаты услуг связи;

— *MAC*-адрес сетевого устройства. Отметим, что установление *MAC*-адреса — необходимая процедура процесса документирования по той причине, что изъятие сетевой техники с идентичным номером *MAC*-адреса при производстве обыска (выемки) является существенным доказательством по уголовному делу.

Необходимо учитывать, что *IP*-адрес может быть как статическим (один адрес соответствуют одному пользователю), так и динамическим (один адрес используется одновременно различными пользователями для подключения к сети). Естественно, что последнее затрудняет установление личности пользователя, однако не делает это невозможным. При получении от провайдеров ответов, содержащих большое количество пользователей, которым выделялся искомый оперативным сотрудником *IP*-адрес, целесообразным является проведение фильтрации ответа с использованием известных сведений (в совокупности с *IP*-адресом обращения, номером телефона, адресом оборудования и др.).

Предоставление динамического *IP*-адреса также характерно для мобильного интернета, то есть с использованием сим-карты оператора сотовой связи. В этом случае следует провести фильтрацию данных с использованием сведений о возможных абонентских номерах телефонов проверяемого лица.

6. Установление принадлежности абонентского номера телефона. Обладая информацией об используемом проверяемым абонентском номере телефона, оперативный сотрудник имеет возможность установить его принадлежность посредством направления мотивированного запроса в адрес компании сотовой связи, без взаимодействия с подразделениями специальных технических мероприятий МВД России (далее — ПСТМ). Полученный ответ может быть представлен в качестве доказательства по уголовному делу, а также содержать в себе, помимо регистрационных данных последнего владельца сим-карты, данные о прежних владельцах, способах пополнения баланса, о платежных операциях по счету.

7. Получение сведений об установочных данных лиц из различных информационных баз данных, поисковых систем, реестров. ОРМ «Наведение справок» проводится также при необходимости установления анкетных данных проверяемых и их связей, используемых средств связи, автомобилей и иных транспортных средств, получения иного характеризующего материала. Для этого целесообразно использовать следующие сервисы информационного обеспечения деятельности:

— ИБД-Ф и ИБД-Р (интегрированный банк данных федерального и регионального уровней). Осуществляется поиск по критериям: лицо, событие (преступление), организация, адрес, автомототранспорт, информация о лице. Кроме того, функционирует модуль оперативно-справочной картотеки (ОСК) — картотеки лиц, подозреваемых или обвиняемых в совершении преступлений, осужденных за совершение преступлений;

— Единая система информационно-аналитического обеспечения деятельности (ИСОД) МВД России, включает такие сервисы, как информационная поисковая система (далее — ИПС) «Следопыт-М», аккумулирующая в себе информацию из различных баз данных, используемых в подразделениях системы МВД России; ФИС «ГИБДД-М», где аккумулируются сведения обо всем зарегистрированном на территории Российской Федерации автотранспорте; АС «Российский паспорт»; АИПС «Оружие-МВД».

Помимо указанных систем, содержат значительный массив информации различные ИПС в области контроля за дорожным движением: ИПС «Андромеда», предоставляющая возможность установления маршрута отдельно взятого автомобиля (с фотографиями), а также ИПС «Паутина».

Добавим, что путем направления запросов в различные государственные и муниципальные органы могут быть установлены сведения об имущественном положении лица, его финансовых обязательствах и задолженностях, имуществе, находящемся в собственности, месте работы, учебы, факте нахождения на специальных учетах в медицинских организациях.

В данном контексте следует упомянуть важнейшее, на наш взгляд, решение законодателя в свете цифровизации общества и противодействия преступности. Федеральным законом от 8 июня 2020 года № 168-ФЗ «О едином федеральном информационном регистре, содержащем сведения о населении Российской Федерации» на базе Федеральной налоговой службы и имеющихся многочисленных разрозненных государственных баз данных и информационных систем создан единый федеральный информационный регистр, содержащий сведения о населении Российской Федерации (далее — ЕФИР). ЕФИР предполагает сбор, обработку, хранение, получение и использование сведений о населении, получаемых из различных баз данных органов исполнительной власти [8].

Сюда следует отнести возможности использования биометрических данных. Федеральным законом от 29 декабря 2022 года № 572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации» [9] утвержден порядок использования Единой биометрической системы (ГИС ЕБС). Система предполагает использование биометрических данных (радужная оболочка глаза, отпечаток пальца, голос, изображение лица, рисунок вен ладони) для идентификации личности в сфере оказания государственных услуг и банковской сфере.

8. Получение сведений на общедоступных ресурсах в сети «Интернет». Необходимо учитывать, что значительный массив сведений может быть получен посредством использования открытых интернет-сервисов, что не требует получения специальных разрешений и санкционирования проведения ОРМ. К таким ресурсам относятся:

— сервисы, позволяющие получить характеризующий материал на проверяемое лицо без направления соответствующих запросов (банк данных исполнительных производств — *https://fssp.gov.ru/iss/ip/*; реестр уведомлений о залоге движимого имущества Федеральной нотариальной палаты — *https://www.reestr-zalogov.ru/*; судебные решения судов общей юрисдикции — судебныерешения.рф, *https://sudact.ru/* и др.);

— сервисы, позволяющие определить банк-эмитент пластиковой карты по БИН (банковский идентификационный номер), оператора связи любого абонентского номера (*http://reg.num*);

— сервисы, позволяющие определить происхождение фотографий и изображений (*http://regex.info/exif.cgi, http://www.findexif.com*);

— сервисы, позволяющие идентифицировать пользователя сети «Интернет» по его имени, номеру телефона или адресу электронной почты (*https://pipl.com, http://www.webmii.com*);

— сервисы, позволяющие получить информацию о владельце доменного имени, хостинг-провайдере, владельце *IP*-адреса (*http://who.is, http://www.whoishostingthis.com, http://myip.ms, http://www.ewhois.com*).

Подводя промежуточные итоги, отметим важное, на наш взгляд, обстоятельство, определяющее определенную научную новизну и практическую направленность нашего исследования. Все вышеуказанные направления проведения ОРМ «Наведение справок» могут осуществляться самостоятельно сотрудниками оперативных подразделений ОВД без привлечения сил и средств ПСТМ МВД России, взаимодействие с которыми затрудняется формально определенными требованиями ведомственных нормативных правовых актов, а полученные результаты проведения оперативно-технических мероприятий, по сути, ничем не отличаются от результатов, полученных при проведении гласного ОРМ «Наведение справок». В этой связи отсутствует необходимость согласования возможности предоставления результатов в органы дознания, следствия и суда, а решение при этом принимает самостоятельно должностное лицо оперативного подразделения ОВД.

Таким образом, рассмотренные нами способы проведения ОРМ «Наведение справок», безусловно, не являются исчерпывающими, но могут отражать основные направления работы сотрудников оперативных подразделений ОВД при выявлении, раскрытии и (или) документировании преступлений, совершаемых как в сети «Интернет», так и преступлений, совершаемых без применения информационно-телекоммуникационных технологий, но выявление и раскрытие которых требуют использования информационно-телекоммуникационных технологий.

В проведенном исследовании нами продемонстрирован широчайший инструментарий ОРМ «Наведение справок» как при обращении к различным автоматизированным информационно-поисковым системам, так и при поиске, сборе, анализе информации о проверяемых лицах с применением информационно-телекоммуникационных сетей. Использование указанных нами способов проведения ОРМ «Наведение справок», уяснение их содержания, а также знание «выходного результата» — конкретной оперативно значимой информации, которую возможно получить, позволят успешно выполнять задачи, стоящие перед ОРД в условиях современного информационного общества.

Список источников

1. Шаров В. И. Оперативно-розыскные мероприятия в сети Интернет // Общество и право. 2018. № 2 (64). С. 82–87.

2. Захаров Н. Д. Деятельность оперативных подразделений органов внутренних дел по выявлению и раскрытию преступлений против половой неприкосновенности несовершеннолетних, совершенных с использованием сети Интернет: дис. … канд. юрид. наук. Волгоград, 2022. 238 с.

3. Захаров Н. Д. Особенности проведения отдельных оперативно-разыскных мероприятий при выявлении и раскрытии преступлений против половой неприкосновенности несовершеннолетних, совершенных с использованием сети Интернет // Вестник Волгоградской академии МВД России. 2023. № 1 (64). С. 108–115.

4. Гаврилин Ю. В., Аносов А. В., Баранов В. В. Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий: учебное пособие: в 2 ч. Ч. 1. Москва: Академия управления Министерства внутренних дел Российской Федерации, 2019. 208 с.

5. Захаров Н. Д. Оперативно-розыскная деятельность в сети Интернет как объект правового регулирования // Оперативно-розыскная деятельность в современных условиях: материалы межведомственной научно-практической конференции, Санкт-Петербург, 22–23 июня 2023 года. Санкт-Петербург: Санкт-Петербургский университет МВД России, 2023. С. 57–61.

6. О деятельности иностранных лиц в информационно-телекоммуникационной сети «Интернет» на территории Российской Федерации: федеральный закон от 1 июля 2021 года № 236-ФЗ. Доступ из СПС «КонсультантПлюс» (дата обращения: 16.01.2024).

7. О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма: федеральный закон от 7 августа 2001 года № 115-ФЗ. Доступ из СПС «КонсультантПлюс» (дата обращения: 16.01.2024).

8. О едином федеральном информационном регистре, содержащем сведения о населении Российской Федерации: федеральный закон от 8 июня 2020 года № 168-ФЗ. Доступ из СПС «Консультант-Плюс» (дата обращения: 16.01.2024).

9. Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации: федеральный закон от 29 декабря 2022 года № 572-ФЗ. Доступ из СПС «Консультант-Плюс» (дата обращения: 16.01.2024).

References

1. Sharov V. I. Operational investigative measures on the Internet. *Society and law*, 2018, no. 2 (64), pp. 82–87. (In Russ.)

2. Zakharov N. D. The activities of the operational units of the internal affairs bodies for the identification and disclosure of crimes against the sexual integrity of minors committed using the Internet. Dissertation... candidate of legal sciences. Volgograd, 2022. 238 p. (In Russ.)

3. Zakharov N. D. Peculiarities of carrying out certain operational investigative measures in the identification and disclosure of crimes against the sexual integrity of minors committed using the Internet. *Bulletin of the Volgograd Academy of the Ministry of Internal Affairs of Russia*, 2023, no. 1 (64), pp. 108–115. (In Russ.)

4. Gavrilin Yu. V., Anosov A. V., Baranov V. V. The activities of the internal affairs bodies to combat crimes committed using information, communication and high technologies: a textbook. In 2 parts. Part 1. Moscow: Academy of Management of the Ministry of Internal Affairs of the Russian Federation Publ., 2019. 208 p. (In Russ.)

5. Zakharov N. D. Operational investigative activity on the Internet as an object of legal regulation. Operational investigative activity in modern conditions: materials of the interdepartmental scientific and practical conference, St. Petersburg, June 22–23, 2023. St. Petersburg: St. Petersburg University of the Ministry of Internal Affairs of Russia, 2023. Pp. 57–61. (In Russ.)

6. On the activities of foreign persons in the information and telecommunications network “Internet” on the territory of the Russian Federation: federal law no. 236-FZ of July 1, 2021. Access from the reference legal system “ConsultantPlus” (accessed 16.01.2024). (In Russ.)

7. On Countering the Legalization (Laundering) of Proceeds from Crime and the Financing of Terrorism: federal law no. 115 FZ of August 7, 2001. Access from the reference legal system “ConsultantPlus” (accessed 16.01.2024). (In Russ.)

8. On the Unified Federal Information Register containing information about the population of the Russian Federation: federal law no. 168-FZ of June 8, 2020. Access from the reference legal system “ConsultantPlus” (accessed 16.01.2024). (In Russ.)

9. On the identification and (or) authentication of Individuals using biometric personal data, on Amendments to Certain Legislative Acts of the Russian Federation and invalidation of Certain Provisions of Legislative Acts of the Russian Federation: federal law no. 572-FZ of December 29, 2022. Access from the reference legal system “ConsultantPlus” (accessed 16.01.2024). (In Russ.)

Информация об авторе

Н. Д. Захаров — кандидат юридических наук, начальник научно-исследовательского отдела Волгоградской академии МВД России.

Information about the author

N. D. Zakharov — Candidate of Sciences (Law), Head of the Research Department of the Volgograd Academy of the Ministry of Internal Affairs of the Russian Federation.