

О НЕКОТОРЫХ НАПРАВЛЕНИЯХ ЦИФРОВИЗАЦИИ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ

Автором статьи указывается на значительные изменения преступности ввиду использования при совершении преступлений новых информационных технологий. Рассматриваются возможности вовлечения достижений информационных технологий в криминалистическую деятельность правоохранительных органов. В статье кратко описаны внедренные системы информационного обеспечения деятельности правоохранительных органов. Описаны направления возможной информатизации деятельности субъектов раскрытия и расследования преступлений на современном этапе. Автором предложены алгоритмы реализации решений по информатизации процессов собирания и фиксации криминалистически значимой информации. Особое внимание уделено дистанционным технологиям проведения следственных действия и оперативно-розыскных мероприятий, а также исследования цифровых носителей. Приведены примеры цифровых механизмов дистанционной идентификации личности и результатов процессуальных действий. Анализируются проблемы применения электронной подписи в совокупности с другими инструментами процесса удостоверения личности пользователя.

Ключевые слова: электронная подпись, расследование преступлений, цифровой носитель информации, следственное действие, криминалистическая деятельность.

A.A. Rudykh

ON SOME TRENDS IN THE DIGITIZATION OF CRIME INVESTIGATION

The author points out that the criminal situation has changed considerably due to the use of new information technologies to commit crimes. The author analyzes the possibility of applying the progress of information technologies to the criminalistic work of the law enforcement bodies. The paper contains a brief overview of the information support of the work of law enforcement bodies. It describes the directions of possible digitization of crime investigation and detection in modern conditions. The author presents algorithms of implementing decisions on the IT support for the collection and recording of criminalistically relevant information. Special attention is paid to the remote work technologies of conducting investigation and operative-search activities as well as the analysis of digital data storage devices. The author presents the examples of digital mechanisms for the long distance identification of persons and the results of procedural actions. He analyzes the problems of using the electronic signature together with other instruments of verifying the personality of the user.

Keywords: electronic signature, investigation of crimes, digital data storage, investigative action, forensic activity.

Цифровые технологии глубоко интегрировались в повседневную жизнь современного общества. Большинство людей не представляют свою жизнь без использования глобальной сети и цифровых устройств. С помощью информационных технологий мы получаем новую информацию, выполняем профессиональную деятельность, следим за здоровьем, совершаем покупки и многое другое. Именно эффективность и ускорение ранее трудоемких процессов сделали популярным информатизацию различных видов человеческой деятельности. На вооружение цифровые технологии были взяты и преступным миром. Повсеместное использование современных технических средств и глобальная информатизация приводят к тому, что классические формы преступности — воровство, грабеж, убийства, мошенничество — уступают место качественно иной преступности [1, с. 255]. Об этом говорят изменения, произошедшие в структуре зарегистрированных преступлений. Только за последние несколько лет, в Уголовный кодекс Российской Федерации был внесен ряд изменений и дополнений. Все больше статей особенной части включают признак совершения преступления с использованием «информационно-телекоммуникационных сетей (включая сеть Интернет)» и т.п. Однако, такими квалифицированными составами преступлений использование информационных технологий в противоправной деятельности не ограничивается. В настоящее время, внушительное количество преступлений, которые ранее совершались «традиционно», происходят дистанционно. Сегодня, сотрудников правоохранительных органов уже трудно удивить случаями краж, мошенничеств, сбытом наркотических веществ или развратных действий в отношении несовершеннолетних, совершенных с использованием глобальной сети удаленно. Очевидно, наметившаяся тенденция видоизменения преступности поднимает вопрос относительно цифровых решений, которые может противопоставить правоохранительная система современной преступности. Информатизация МВД России не стоит на месте, по мере развития технологий постоянно обновляет свою инфраструктуру техническое оборудование, автоматизированные системы, систему безопасности [2, с. 112]. В частности, в целях реализации конституционных прав граждан на обращение в государственные органы, функционирует система принятия и регистрации обращений граждан в электронном виде. Это позволяет оперативно получать информацию от граждан и реагировать на обращения. Также, развиваются внутренние информационные системы обеспечения деятельности правоохранительных органов. Одно из успешно реализованных решений — система информационно-аналитического обеспечения деятельности (ИСОД) МВД России. Она состоит из десятков информационных сервисов для

решения ключевых задач подразделений полиции на всей территории Российской Федерации¹. Указанную систему можно отнести к сегменту информационно-справочного обеспечения деятельности по раскрытию и расследованию преступлений. Специфика использования при расследовании преступлений информационных технологий состоит в том, что их внедрение возможно на каждой стадии судопроизводства – от регистрации полученной исходной информации до судебного заседания, где уже практикуется применение систем видеоконференций, участники данного соединения находятся в разных населенных пунктах, при этом могут поддерживать прямой интерактивный диалог [3, с. 140]. Использование дистанционных технологий, как показывает зарубежный опыт, не ограничивается вопросами раскрытия преступлений, они применяются и в обучении сотрудников правоохранительных органов [4, с. 493].

В настоящее время, интересным представляется вопрос о рассмотрении подходов в применении и использовании цифровых технологий непосредственно при организации процесса поиска и фиксации криминалистически значимой информации. Уголовно-процессуальный кодекс Российской Федерации предусматривает применение технических средств при производстве следственных действий. Сегодня, субъекты расследования нередко прибегают к применению компьютерной техники подключенной к сети Интернет для проведения осмотра и поиска информации на удаленных информационных ресурсах, предлагаются даже методики для работы следователя в сети Интернет [5, с. 139]. По такому алгоритму, зачастую исследуются отдельные сайты, информация, находящаяся в электронной почте, страницы в социальных сетях, и прочий информационный контент, расположенный на удаленных технических площадях. Эта методика позволяет не только отыскать криминалистически значимую информацию, находящуюся за пределами кабинета следователя, но и зафиксировать ее, путем отражения в протоколе следственного действия или копирования на цифровой носитель информации. Одним из эффективных способов фиксации и отображения хода осмотра, является технология снимка экрана «скриншот», которая позволяет запечатлеть информацию, отображенную на дисплее компьютера и зафиксировать ее в приложении к протоколу следственного действия. Некоторые авторы, предлагают заверять такие снимки при помощи специальных программ [6, с. 54].

Удаленный доступ к информации на сегодняшний день применяется, как правило, для проведения следственного осмотра и оперативно-розыскных мероприятий, связанных с поиском и фиксацией информации находящийся на удаленных ресурсах. Тем не менее, подробной методики регламентирующей порядок и границы проведения процессуальных действий по удаленному отысканию и фиксации компьютерной информации, в настоящее время, не имеется. К сожалению, отсутствие в УПК РФ, норм, регламентирующих основания, порядок и

¹ Центр информационных технологий, связи и защиты информации ГУ МВД России по Иркутской области информирует // Главное управление МВД России по Иркутской области. 2018. URL: <https://38.мвд.рф/news/item/13485814/>.

особенности удаленного (дистанционного) исследования компьютерной информации при расследовании преступлений, является существенным пробелом, ограничивающим деятельность следователя по собиранию доказательств [7, с. 75]. Вместе с тем, в условиях развития преступности необходимо рассмотрение вопроса о внедрении в практику правоохранительных органов возможности дистанционного добывания информации не только из сети Интернет. В то время, когда преступники «успешно» используют достижения технического прогресса, и совершают преступления, находясь в сотнях или тысячах километрах от потерпевшего, криминалистическая деятельность продолжает оставаться традиционно контактной, что заведомо создает неравные условия.

Особенностью преступлений, связанных с использованием информационных технологий является территориальная удаленность относительно друг друга участников событий, а также удаленное местонахождение носителей информации, имеющей значение для уголовного дела. Зачастую, участники уголовного процесса находятся в разных городах или даже странах. При таких условиях, проведение необходимых оперативно-розыскных и процессуальных действий становятся настоящим испытанием для субъекта расследования. В качестве примера, можно рассмотреть достаточно распространенную сегодня ситуацию, связанную с расследованием мошенничества совершенного дистанционным способом. В этом случае, пострадавший, нередко, в целях защиты своих прав, с использованием сети Интернет, дистанционно обращается в правоохранительные органы. Обращение поступает в территориальный орган внутренних дел, с территории обслуживания которого, по мнению пострадавшего, осуществлялись противоправные действия. В указанной первоначальной следственной ситуации субъекту расследования преступления необходимо допросить потерпевшего и признать его таковым, в соответствии с действующим уголовно-процессуальным законодательством. Также, необходимо произвести осмотр цифровых носителей информации находящейся у потерпевшего. Кроме того, для эффективного раскрытия и расследования преступления следует истребовать информацию от Интернет-сервиса обмена информацией. В связи с тем, что потерпевший и источники информации находится в разных регионах, на выполнения необходимых действий требуется значительное время.

Рассмотренный пример обнаруживает устарелость существующей методики расследование дистанционных преступлений. Фактически правоохранительные органы к противодействию преступлениям в сфере информационных технологий с их экстерриториальной особенностью оказались малоподготовленными, в виду использования классических контактных методов сбора и фиксации информации.

Многие авторы исследовали вопросы, связанные с необходимостью внедрения в практику дистанционной деятельности по раскрытию и расследованию преступлений. Подвергались анализу возможности удаленного проведения разных следственных действий. Так, Смагин П.Г. в качестве аргумента к внедрению такой методики приводит положительный опыт дистанционных следственных действий органов расследования зарубежных стран [8, с. 309]. По нашему мнению, раскрытие современных преступлений совершенных дистанционно требует

применения аналогичных технологий расследования. Этот подход к формированию новых направлений информатизации криминалистической деятельности представляется адекватным и эффективным ответом на складывающуюся действительность. Цифровизация деятельности субъектов расследования должна основываться на возможности дистанционного (удаленного) собирания и фиксации доказательств. Некоторые авторы, исследующие темы оснащения криминалистической деятельности дистанционным инструментарием приходят к выводу о том, что для реализации этого решения требуются: помещения, технические комплексы и персонал. Например, Кравец Е.Г. указывает, что для использования информационно-коммуникационных технологий при производстве следственных действий необходимы оборудованные специализированные помещения для дистанционных сеансов. Связь с удаленным пунктом, реализацию технических мероприятий осуществляют сотрудники подразделений информационного обеспечения, прошедшие специальную подготовку по организации сеансов видеоконференцсвязи [9, с. 140]. В целом, разделяя эту точку зрения, необходимо добавить, что технический прогресс не стоит на месте, и некоторые системы программно-технических средств, которые потенциально могут быть использованы в раскрытии преступлений, уже сформировались.

При существующем уровне технического оснащения общества, возможно, уже нет необходимости создавать специальную систему технических средств, помещений, обслуживающего персонала для обеспечения реализации удаленного собирания и закрепления доказательств. Человек, в настоящее время, совершает широкий перечень юридически значимых действий с использованием информационно-телекоммуникационной сети Интернет. В частности, сегодня, доступно дистанционно зарегистрировать юридическое лицо, предоставить отчетность в налоговые органы с использованием электронно-цифровой подписи, направить в электронном виде процессуальные документы в суд и т.д. Подавляющее большинство людей имеют в своем распоряжении одно или несколько цифровых устройств отвечающих необходимым требованиям функциональности. В этих условиях, процесс формирования инструментария для дистанционной деятельности по обнаружению, фиксации доказательств может развиваться по трем основным направлениям. Первое, это технология дистанционного получения информации от организаций. Расследование подавляющего большинства преступлений, связанных с использованием информационных технологий, включает необходимость получения информации от различных организаций. К ним относятся: операторы связи и организаторы распространения информации, в базах данных, которых, хранится информация, перечень которой предусмотрен ст. 64 «ФЗ О связи»², и ст. 10.1 ФЗ «Об Информации, информационных технологиях и о защите информации»³, кредитно-финансовые организации, операторы

² О связи :федер. закон от 7 июля 2003 г. № 126-ФЗ // Собрание законодательства РФ. 2003. № 28. Ст. 2895.

³ Об информации, информационных технологиях и о защите информации :федер. закон от 27 июля 2006 г. 149-ФЗ // Собрание законодательства РФ. 2006. № 31 (1 ч.). Ст. 3448.

электронных платежных систем, налоговые органы, пенсионный фонд, учреждения здравоохранения и т.д. Обеспечение возможности сетевого запроса информации этих организаций, позволит в короткий промежуток времени, при соблюдении юридических условий, требований конфиденциальности и оснований доступа, получить сведения имеющие значения для расследования.

Вторым важным направлением развития дистанционной криминалистической деятельности, является внедрение технологии удаленного исследования различных объектов. Такими объектами могут быть: места происшествий, отдельные физические предметы, информационные ресурсы, файлы в информационном пространстве, цифровые носители информации. Некоторые перечисленные методики уже применяются в практической деятельности правоохранительных органов, например, удаленный осмотр ресурсов в сети Интернет. Весьма перспективным представляется вопрос организации удаленного исследования цифровых носителей информации. В настоящее время, носители информации необходимо изымать и транспортировать до экспертного учреждения или специалиста, обладающего требуемыми технологиями исследования. Все это, приводит к финансовым и временным затратам и создает опасность утраты информации при несвоевременном изъятии или некачественной транспортировке. Вместо этого, используя каналы связи, достаточно подключить носитель информации к сети и эксперт, находящийся в другом регионе или стране может осуществить необходимые исследования информации.

Третьим направлением цифровизации деятельности по расследованию преступлений, является внедрение механизмов удаленного получения информации от физических лиц. Большинство людей постоянно носят с собой цифровые средства коммуникации для общения между собой, данные средства используются для реализации гражданских прав, обращения в государственные органы, совершение юридически значимых действий с использованием официальных Интернет-порталов. Повсеместно, клиенты банков при помощи специального программного приложения, осуществляют управление своим счетом через смартфон или персональный компьютер. Закономерно возникает вопрос, почему же тогда, до сих пор не реализована возможность дистанционного опроса очевидца происшествия или, к примеру, допроса потерпевшего в рамках расследования уголовного дела. Некоторые авторы уже поднимали вопрос о необходимости совершенствования технологий взаимодействия следователя с общественностью [10, с. 181].

Сравнительный анализ дистанционного способа расследования преступления и юридически значимых действий, которые уже возможно осуществить в электронном виде, приводит нас к выводу, что среди требований к такой организации деятельности, на первое место выходят вопросы идентификации и аутентификации. В свете рассматриваемой темы, это внедрение технологий надежного установления и подтверждения личности участников дистанционных следственных действий или оперативно-розыскных мероприятий, а также процесс закрепления хода и результатов таких действий.

Вероятным решением развития цифровизации деятельности по расследованию и раскрытию преступлений, может стать использование специально разработанного программного приложения для мобильных цифровых устройств, обеспечивающее взаимодействие пользователя с правоохранительными органами. Первоначальное удостоверение личности, активация учетной записи в приложении, обеспечение пользователя электронной цифровой подписью, может осуществляться в правоохранительных или иных государственных органах по месту проживания лица. Этот этап, допустимо сравнить с получением идентификатора от портала государственных услуг. В возможности приложения могут входить функции обоюдной идентификации личности, как сотрудника правоохранительных органов, так и лица, в отношении которого осуществляется следственное действие или оперативно-розыскное мероприятие. Удостоверение личности может быть осуществлено с использованием многофакторной аутентификации, например, парольной защиты, голосовой идентификации, идентификации по лицу, по отпечаткам пальцев, sms-подтверждение. Указанное приложение может автоматически заполнять необходимые формы и формировать протокол следственных действий, который в последующем, будет распечатан и приобщен к материалам уголовного дела. Файл с видеотрансляцией процесса дистанционного допроса может быть сохранён, верифицирован и помещен в специально созданный, на основе технологии «блокчейн»⁴, защищенный массив данных. В случае необходимости, в рамках дальнейшего расследования, либо судебного рассмотрения, указанный файл может быть просмотрен и проверен на предмет соответствия информации, отражённой в протоколе, ходу и результатам следственного действия. Предлагаемая технология позволит не только оперативно проводить удаленные допросы лиц, но и обеспечит достоверность и допустимость результатов следственного действия в силу его прозрачности и проверяемости на любой стадии судебного преследования.

Процесс удостоверения протокола следственного действия, может быть осуществлен с использованием усиленной квалифицированной электронной подписи⁵. Первые шаги применения электронной подписи в уголовном судопроизводстве, связаны с введением в действие ст. 474.1 УПК РФ, в соответствии с которой, судам разрешено изготавливать судебные решения в электронной форме и подписывать их усиленной квалифицированной электронной подписью. Проблемы применения электронной подписи в правоприменительной деятельности уже исследовались. Так, Сударикова Т.Е. указывает на то, что одной из проблем является тот факт, что поскольку уголовный процесс в большей мере, чем иной ограничивает личные права подозреваемого, обвиняемого, а также, учитывая специфику производства многих следственных и процессуальных действий, возможность применять электронные документы сужена. Исходя из этого, мы можем прийти к выводу, что в сфере уголовного процесса практически нет

⁴Блокчейн // Википедия. Свободная энциклопедия. URL: <https://ru.wikipedia.org/wiki/Блокчейн>.

⁵ Об электронной подписи :федер. закон от 6 апр. 2011 г. № 63-ФЗ // Собрание законодательства РФ. 2011. № 15. Ст. 2036.

возможности заверить документ электронной цифровой подписью и другими аналогами собственноручной подписи [11, с. 101]. Выводы автора, безусловно, имеют под собой основания. Известны случаи неправомерного использования электронной подписи. Однако, по нашему мнению, исследование вопросов использования электронной подписи в рамках правоохранительной деятельности является весьма перспективным направлением. Здесь, следует уделить внимание использованию технологий электронной подписи совместно с другими вышеназванными способами аутентификации, что позволит свести к минимуму какие-либо фальсификации и обеспечит прозрачность и проверяемость любых действий участников уголовного процесса и субъекта расследования. В настоящее время уже имеются решения позволяющие использовать усиленную квалифицированную электронную подпись в смартфонах и других персональных устройствах.⁶ Безусловно, эти решения требуют глубокой юридической и технологической проработки, однако для них не требуется огромного финансирования, а их эффективность позволит продвинуться в совершенствовании механизмов противодействия преступности.

Список использованной литературы

1. Савельева М.В. Технологизация криминалистики / М.В. Савельева, А.Б. Смушкин // Вестник Саратовской государственной юридической академии. – 2017. – № 5 (118). – С. 254–257.
2. Стрижченко И.А. Единая информационно телекоммуникационная система в ОВД / И.А. Стрижченко, Б.Н. Тюрбеев // Современные проблемы обеспечения охраны общественного порядка при проведении массовых мероприятий. Пресечение массовых беспорядков : материалы регионального межведомственного науч.-практ. семинара, Волгоград, 18 нояб. 2015 г. – Москва, 2015. – С. 108–113.
3. Кравец Е.Г. Дистанционные следственные действия сквозь призму применения специальных знаний / Е.Г. Кравец, Н.В. Шувалов // Юридическая наука и правоохранительная практика. – 2017. – № 1 (39). – С.140–144.
4. Муратова Е.Н. Возможности «Виртуального отдела полиции» в реализации уголовной политики (из опыта полиции ФРГ) / Е.Н. Муратова // Приоритетные направления развития науки и образования. – 2015. – № 2 (5). – С. 493–495.
5. Гамбарова Е.А. К вопросу о методике использования социальных сетей в работе следователя / Е.А. Гамбарова // Юридический вестник Самарского университета. – 2017. – № 3. – С. 137–141.
6. Юношев С.В. К проблеме процессуального оформления доказательственной информации, полученной из Интернет-источников / С.В. Юношев,

⁶ Компания "Аладдин Р.Д." сообщает о начале продаж новых SecureMicroSD-токенов JaCarta, сертифицированных ФСБ России // Аладдин. URL: https://www.aladdin-rd.ru/company/press-room/news/kompania_aladdin_rd_soobsaet_o_nacale_prodaz_novyh_secure_microsd_tokenov_jacarta_sertificirovannyh_fsb_rossii.

С.В. Кондратюк // Вектор науки Тольяттинского государственного университета. Серия: Юридические науки. – 2018. – № 3. – С. 52–57.

7. Иванов А.И. Удаленное исследование компьютерной информации: уголовно-процессуальные и криминалистические проблемы / А.И. Иванов // Известия Саратовского университета. Новая серия. Серия: Экономика. Управление. Право. – 2009. – Т. 9, № 2. – С. 75–77.

8. Смагин П.Г. К вопросу о возможности дистанционного производства следственных действий / П.Г. Смагин // Уголовно-процессуальные и криминалистические проблемы борьбы с преступностью : Всероссийская науч.-практ. конф., Орел, 29 мая 2015 г. – Орел, 2015. – С. 309–314.

9. Кравец Е.Г. Дистанционные следственные действия сквозь призму применения специальных знаний / Е.Г. Кравец, Н.В. Шувалов // Юридическая наука и правоохранительная практика. – 2017. – № 1 (39). – С. 140–144.

10. Богомолова А.Г. Факторы определяющие выбор средств и технологий взаимодействия следователя с общественностью / А.Г. Богомолова // Вестник Восточно-Сибирского института МВД России. – 2018. – № 4 (87). – С. 180–185.

11. Сударикова Т.Е. Электронная подпись в уголовном процессе РФ / Т.Е. Сударикова // Организационное, процессуальное и криминалистическое обеспечение уголовного производства : материалы VI Междунар. науч. конф. студентов и магистрантов. – Симферополь, 2017. – С. 101–103.

References

1. Savelieva M.V., Smushkin A.B. Criminalistics Technologizing. *Vestnik-Saratovskoi gosudarstvennoi yuridicheskoi akademii = Bulletin of Saratov State Law Academy*, 2017, no. 5 (118), pp. 254–257. (In Russian).

2. Strizhchenko I.A., Tyurbeyev B.N. Unified information telecommunication system in the police department. *Sovremennye problem obespecheniya okhrany obshchestvennogo poryadka pri provedenii massovykh meropriyatii. Presechenie massovykh besporyadkov. Materialy regional'nogo mezhvedomstvennogo nauchno-prakticheskogo seminara, Volgograd, 18 noyabrya 2015 g.* [Modern Problems of providing the protection of public order during mass events. Suppression of mass disorder. Regional Inter-Departmental Research and Practice Workshop Materials, Volgograd, November, 18, 2015]. Moscow, 2015, pp. 108–113. (In Russian).

3. Kravets E.G., Shuvalov N.V. Distance Investigative Actions through the Application of Special Knowledge. *Yuridicheskaya nauka i pravookhranitel'naya praktika = Legal Science and Law Enforcement Practice*, 2017, no. 1 (39), pp. 140–144. (In Russian).

4. Muratova E.N. The possibility of the “Virtual Police Department” in the implementation of criminal policy (from the experience of the FRG police). *Prioritetnye napravleniya razvitiya nauki i obrazovaniya = Priority Directions of Science and Education Development*, 2015, no. 2 (5), pp. 493–495. (In Russian).

5. Gambarova E.A. Technique of Using Social Networks in the Work of an Investigator. *Yuridicheskii vestnik Samarskogo universiteta = Juridical Journal of Samara University*, 2017, no. 3, pp. 137–141. (In Russian).

6. Yunoshev S.V., Kondratyuk S.V. Concerning the Issue of Procedural Implementation of the Evidentiary Information Acquired from the Internet Sources. *Vektor nauki Tolyattinskogo gosudarstvennogo universiteta Seriya: Yuridicheskie nauki = Science Vector of Togliatti State University. Series: Legal Sciences*, 2018, no. 3, pp. 52–57. (In Russian).

7. Ivanov A.N. Remote Study of Computer Information: Criminal Procedure and Forensic Problems. *Izvestiya Saratovskogo universiteta. Novaya seriya. Seriya: Ekonomika. Upravlenie. Pravo = Izvestiya of Saratov University. New Series. Series: Economics. Management. Law*, 2009, vol. 9, no. 2, pp. 75–77. (In Russian).

8. Smagin P.G. To the problem of the possibility of remote investigative work. *Ugolovno-protsessual'nye i kriminalisticheskie problem bor'by s prestupnost'yu. Vserossiiskaya nauchno-prakticheskaya konferentsiya, Orel, 29 maya 2015 g.* [Criminal Procedure and Criminalistic Problems of Counteracting Crime. All-Russian Research Conference, Orel, May, 29, 2015]. Orel, 2015, pp. 309–314. (In Russian).

9. Kravets E.G., Shuvalov N.V. Distance Investigative Actions through the Application of Special Knowledge. *Yuridicheskaya nauka i pravookhranitel'naya praktika = Legal Science and Law Enforcement Practice*, 2017, no. 1 (39), pp. 140–144. (In Russian).

10. Bogomolova A.G. Factors Determining the Selection of the Means and Technologies of the Interaction of the Public Investigator. *Vestnik Vostochno-Sibirskogo instituta MVD Rossii = Vestnik of the Eastern Siberia Institute of the Ministry of the Interior of the Russian Federation*, 2018, no. 4 (87), pp. 180–185. (In Russian).

11. Sudarikova T.E. Electronic signature in the criminal process in the Russian Federation. *Organizatsionnoe, protsessual'noe i kriminalisticheskoe obespechenie ugolovnogo proizvodstva. Materialy VI Mezhdunarodnoi nauchnoi konferentsii studentov i magistrantov* [Organizational, Procedural and Criminalistic Support of the Criminal Process. Materials of the VI International Scientific Conference]. Simferopol, 2017, pp. 101–103. (In Russian).

Информация об авторе

Рудых Алексей Александрович – аспирант кафедры криминалистики, судебных экспертиз и юридической психологии, Байкальский государственный университет, 664003, г. Иркутск, ул. Ленина, 11; e-mail: irkutianin38@gmail.com

Information about the author

Rudyh, Alexey A. – Ph.D. student, Chair of Criminalistics, Forensic Inquiry and Legal Psychology, Baikal State University, Lenin st., 11, Irkutsk, 664003, the Russian Federation; e-mail: irkutianin38@gmail.com